Exhibit 8

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	Gregory G. Raleigh, et al.
U.S. Patent No.:	9,143,976 Attorney Docket No.: 39843-0158IP1
Issue Date:	September 22, 2015
Appl. Serial No.:	14/676,704
Filing Date:	April 1, 2015
Title:	WIRELESS END-USER DEVICE WITH DIFFERENTIATED NETWORK ACCESS AND ACCESS STATUS FOR BACKGROUND AND FOREGROUND DEVICE APPLICATIONS

DECLARATION OF DR. KEVIN R. B. BUTLER

I hereby declare that all statements made of my own knowledge are true and that all statements made on information and belief are believed to be true. I further declare that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of the Title 18 of the United States Code.

Dated: 2023/08/11

By: KButler

Kevin R. B. Butler, Ph.D.

TABLE OF CONTENTS

I, Kevin R. B. Butler of Gainesville, Florida, declare that:

I. ASSIGNMENT

1. I have been retained on behalf of Samsung Electronics Co., Ltd. (“Samsung”) to offer technical opinions related to U.S. Patent No 9,143,976 (“the ’976 patent”) (SAMSUNG-1001). I understand that Samsung is requesting that the Patent Trial and Appeal Board (“PTAB” or “Board”) to institute an *inter partes* review (“IPR”) proceeding of the ’976 patent.

2. I have been asked to provide my independent analysis of the ’976 patent based on the prior art publications cited in this declaration.

3. I am not and never have been, an employee of Samsung. I received no compensation for this declaration beyond my normal hourly compensation based on my time actually spent analyzing the ’976 patent, the prior art publications cited below, and issues related thereto, and I will not receive any added compensation based on the outcome of any IPR or other proceeding involving the ’976 patent.

II. QUALIFICATIONS

4. I am over the age of 18 and am competent to write this declaration. I have personal knowledge, or have developed knowledge of these technologies based upon education, training, or experience, of the matters set forth herein.

5. I have summarized in this section my educational background, career history, publications, and other relevant qualifications.

6. I received a B.Sc. degree in Electrical Engineering from Queen's University in 1999, an M.S. degree in Electrical Engineering from Columbia University in 2003, and a Ph.D. in Computer Science and Engineering from the Pennsylvania State University in 2010.

7. I am a Professor with tenure in Computer and Information Science and Engineering and Director of the Florida Institute for Cybersecurity Research at the University of Florida. I founded and directed the Oregon Systems Infrastructure and Information Security (OSIRIS) Lab at the University of Oregon, where I was an assistant professor of computer and information science for four years before moving to Florida under the Rising to National Preeminence initiative. I have authored over 115 peer-reviewed publications including book chapters, journal articles, conference proceedings papers, and workshop papers. My research is in the area of computer systems security, including embedded systems, mobile devices, and firmware, as well as network security, including the security of Internet routing and security of telecommunications networks. I received a National Science Foundation CAREER award in 2013, an International Educator of the Year award within the Herbert Wertheim College of Engineering at the University of Florida in 2017, a University of Florida Term Professorship for 2018-2021 and 2021-2024, and an Arnold and Lisa Goldberg Rising Star Endowed Professorship in Computer Science for 2018-2024, which I relinquished in 2021

upon promotion to Full Professor. I also received an Outstanding Community Service Award from the IEEE Technical Committee on Security and Privacy in 2017. I am a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE), and a Senior Member of the Association for Computing Machinery (ACM). I have been involved with international standards-setting bodies; in particular, I was co-chair and leader of the Security Workstream for the International Telecommunications Union (ITU)'s Technology, Innovation, and Competition Working group within the Focus Group on Digital Financial Service from 2015-2016, and from 2017-2022, I served as Co-Chair of the Security, Infrastructure, and Trust Working Group within the ITU's Financial Inclusion Global Initiative. I currently serve on four journal editorial boards, have served on numerous funding panels for the National Science Foundation and reviewed grant proposals on behalf of science and engineering boards in Austria, Canada, and Israel. I have served on over 115 technical program committees for selecting papers to appear at academic conferences on computer security, and I have served as program committee chair and general conference chair for multiple conferences. I have also given over 100 presentations and invited talks, including invited lectures at the University of Oxford, ETH Zurich, the Chinese Academy of Sciences, Dartmouth College, Columbia University, and UCLA. My research has

been featured in news outlets such as the Wall Street Journal, BBC News, and WIRED.

8. I have experience with services and application implementation in communication networks. At Flarion Technologies in 2003, I implemented packet diversion and IP header modification program in the FreeBSD operating system for mobile IP packet testing, to be deployed on WiFi devices. In 2004 at AT&T Labs-Research, I led the design and implementation of mechanisms to support the secure delivery of routing information within the Border Gateway Protocol and evaluated their efficacy using routing data. I have also led the development of a survey of security mechanisms for the Border Gateway Protocol that has been cited over 500 times.

9. I have experience with services and implementation in telecommunication networks, particularly telephony networks. As a research assistant at Columbia University in 2001-2002, I incorporated authentication protocols into a Java-based software stack for the Session Initiation Protocol used for Internet telephony. More recently, I led a project that demonstrated the extraction of data from smartphone firmware images and demonstrated that legacy command sets (i.e., “AT commands” developed for modems in the 1980s) were being used to provide undocumented features on these devices that could be accessed over a USB connection, as well as methods for enabling the transmissions

of these commands. I also led the investigation of the processors on smartphones that are used for communicating with the cellular network and developed an analysis framework that found vulnerabilities in the implementation of cellular communication network protocols implemented in these devices.

10. I have experience with the development and analysis of software and firmware. In 1998 at the Royal Bank of Canada, I developed client-server applications, including design of graphical user interfaces on the client side, to port business processes from mainframe environments.

11. Further, in 2006 I compiled and modified OpenEmbedded firmware to support the SlugOS environment to allow experimentation with storage devices, in order to develop a disk prototype for preventing a type of malware called a rootkit from persisting on a system after reboot. Since then, I have led efforts to analyze firmware on embedded devices, particularly firmware from USB flash drives that uses the Intel 8051 microcontroller, and demonstrated how such binary firmware could be lifted to an intermediate representation to enable control flow graph recovery and symbolic analysis.

12. I have experience with peripherals and portable devices. In 2009, I developed a USB device capable of attesting the integrity of the host computer it was attached to while at Symantec Research. This work was later patented (U.S. Patent 8,856,918, Host validation mechanism for preserving integrity of portable

storage data. Petros Efstathopulos, Bruce Montague, Dharmesh Shah, Kevin Butler. October 7, 2014.). Since then, I have overseen the development of USB devices that allow for tracking the provenance of data at the block level and the development of mobile device software that automates the collection of USB enumeration data.

13. I have also been involved with numerous projects incorporating encryption, such as a mechanisms using additive homomorphic encryption to support accounting audits for preserving the confidentiality of wiretap records and cryptographic schemes for assuring the secure time release of data.

14. My curriculum vitae, attached as Exhibit A, includes a list of publications on which I am a named author. It contains further details regarding my experience, education, publications, and other qualifications provide to an expert opinion in connection with this proceeding.

III. SUMMARY OF CONCLUSIONS FORMED

15. This Declaration explains the conclusions that I have formed based on my analysis. To summarize those conclusions:

- **Ground 1A:** Based upon my knowledge and experience and my review of the prior art publications in this declaration, I believe that claims 1-4, 8-10, 13, 14, 16, 19, 20, 25, 27, and 28 of the ’976 patent are made obvious by Rao and Oestvall.

- **Ground 1B:** Based upon my knowledge and experience and my review of the prior art publications in this declaration, I believe that claims 5-7, 11, 17, 18, 23, 24, 26, and 29 of the ’976 patent are made obvious by Rao, Oestvall, and Montemurro.
- **Ground 1C:** Based upon my knowledge and experience and my review of the prior art publications in this declaration, I believe that claims 12, 15, 21, and 22 of the ’976 patent are made obvious by Rao, Oestvall, and Araujo.

IV. LEVEL OF ORDINARY SKILL IN THE ART

16. I have been informed that a person of ordinary skill in the art (“POSITA”) is a hypothetical person who is presumed to have the skill and experience of an ordinary worker in the field at the time of the alleged invention. The ’976 patent was filed April 1, 2015, and claims priority to several provisional applications, the earliest of which was filed January 28, 2009 (“Critical Date”). Because I do not know at what date the invention as claimed was made, if ever, I have used the Critical Date of the ’976 patent as the point in time for claim interpretation purposes. My opinion does not change if the invention date is earlier.

17. Based on my knowledge and experience in the field and my review of the ’976 patent and file history, I believe that a person of ordinary skill in the art in this matter would have had (1) at least a bachelor’s degree in computer science,

computer engineering, electrical engineering, or a related field, and (2) at least two years of industry experience in services and application implementation in communication networks. Additional graduate education could substitute for professional experience, and vice versa. Based on my experiences, I have a good understanding of the capabilities of a POSITA. Indeed, I have taught, mentored, advised, and collaborated closely with many such individuals over the course of my career.

V. LEGAL PRINCIPLES

18. I am not a lawyer and I will not provide any legal opinions in this IPR. Although not a lawyer, I have been advised that certain legal standards are to be applied by technical experts in forming opinions regarding the meaning and validity of patent claims.

A. Terminology

19. I understand that claim terms are generally given their plain and ordinary meaning based on the patent's specification and file history as understood by a person of ordinary skill in the art at the time of the purported invention. In that regard, I understand that the best indicator of claim meaning is its usage in the context of the patent specification as understood by a POSITA. I further understand that the words of the claims should be given their plain meaning unless that meaning is inconsistent with the patent specification or the patent's history of

examination before the Patent Office. I also understand that the words of the claims should be interpreted as they would have been interpreted by a POSITA at the time of the invention was made (not today).

B. Priority

20. I understand that a continuation application is a later-filed application that has the same disclosure (specification and figures) as an earlier filed application to which the later-filed application claims priority. A continuation is generally entitled to the same priority date as the later-filed application to which it claims priority.

C. Anticipation

21. I have been informed that a patent claim is invalid as anticipated under 35 U.S.C. § 102 if each and every element of a claim, as properly construed, is found either explicitly or inherently in a single prior art reference. Under the principles of inherency, if the prior art necessarily functions in accordance with, or includes the claimed limitations, it anticipates.

22. I have been informed that a claim is invalid under 35 U.S.C. § 102(a) if the claimed invention was known or used by others in the U.S., or was patented or published anywhere, before the applicant's invention. I further have been informed that a claim is invalid under 35 U.S.C. § 102(b) if the invention was patented or published anywhere, or was in public use, on sale, or offered for sale in

this country, more than one year prior to the filing date of the patent application (critical date). And a claim is invalid, as I have been informed, under 35 U.S.C. § 102(e), if an invention described by that claim was described in a U.S. patent granted on an application for a patent by another that was filed in the U.S. before the date of invention for such a claim.

D. Obviousness

23. I have been informed that a patent claim is invalid as "obvious" under 35 U.S.C. § 103 in light of one or more prior art references if it would have been obvious to a POSITA, taking into account (1) the scope and content of the prior art, (2) the differences between the prior art and the claims, (3) the level of ordinary skill in the art, and (4) any so called "secondary considerations" of nonobviousness, which include: (i) "long felt need" for the claimed invention, (ii) commercial success attributable to the claimed invention, (iii) unexpected results of the claimed invention, and (iv) "copying" of the claimed invention by others.

24. For purposes of my analysis above and because I know of no indication from the patent owner or others to the contrary, I have applied a date of January 28, 2009, as the date of invention in my obviousness analyses, although in many cases the same analysis would hold true even at an earlier time than January 28, 2009.

25. I have been informed that a claim can be obvious in light of a single prior art reference or multiple prior art references. To be obvious in light of a single prior art reference or multiple prior art references, there must be a reason to modify the single prior art reference, or combine two or more references, in order to achieve the claimed invention. This reason may come from a teaching, suggestion, or motivation to combine, or may come from the reference or references themselves, the knowledge or "common sense" of one skilled in the art, or from the nature of the problem to be solved, and may be explicit or implicit from the prior art as a whole.

26. I have been informed that the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. I also understand it is improper to rely on hindsight in making the obviousness determination.

27. To the extent these factors have been brought to my attention, if at all, I have taken them into consideration in providing my opinions and conclusions.

VI. MATERIALS CONSIDERED

28. My analysis and conclusions set forth in this declaration are based on my educational background and experiences in the field (*see* Section II). Based on my knowledge and experience, I believe that I am considered to be an expert in the field. Also, based on my knowledge and experience, I understand and know of the

capabilities of persons of ordinary skill in the field during the early 2000s–2010s, and I taught, participated in organizations, and worked closely with many such persons in the field during that time frame.

29. As part of my independent analysis for this declaration, I have considered the following: the background knowledge/technologies that were commonly known to persons of ordinary skill in this art during the time before the earliest claimed priority date for the ’976 patent; my own knowledge and experiences gained from my work experience in the field of the ’ 976 patent and related disciplines; and my experience in working with others involved in this field and related disciplines.

30. In addition, I have analyzed the following publications and materials:

- U.S. Patent No. 9,143,976 to Raleigh, et al. (“the ‘976 Patent”) (SAMSUNG-1001)
- Complaint for Patent Infringement in *Headwater Research LLC v. Samsung Electronics Co., Ltd. et al.*, 2:22-cv-00467 (E.D. Tex. Dec. 6, 2022) (SAMSUNG-1004)
- U.S. Pat. App. Pub. No. 2006/0039354 (“Rao”) (SAMSUNG-1005)
- U.S. Pat. App. Pub. No. 2007/0038763 (“Oestvall”) (SAMSUNG-1006)

- U.S. Pat. App. Pub. No. 2009/0207817 ("Montemurro") (SAMSUNG-1007)
- U.S. Pat. App. Pub. No. 2008/0080458 ("Cole") (SAMSUNG-1009)
- U.S. Pat. No. 5,987,611 ("Freund") (SAMSUNG-1010)
- U.S. Pat. App. Pub. No. 2009/0217065 ("Araujo") (SAMSUNG-1011)
- U.S. Pat. App. Pub. No. 2010/0115048 ("Scahill") (SAMSUNG-1012)
- U.S. Pat. No. 8,381,127 ("Singh") (SAMSUNG-1013)
- U.S. Pat. App. Pub. No. 20070173283A1 ("Livet") (SAMSUNG-1014)
- U.S. Pat. No. 8,413,172 ("Sng") (SAMSUNG-1015)
- Flinn, Jason, et al. "The case for intentional networking," Proceedings of the 10th Workshop on Mobile Computing Systems and Applications, 2009 ("Flinn") (SAMSUNG-1016)
- Carter, Casey et al., "Contact networking: a localized mobility system," Proceedings of the 1st International Conference on Mobile systems, Applications and Ser-vices, 2003 ("Carter") (SAMSUNG-1017)

- U.S. Pat. No. 8,407,345 to Lim ("Lim") (SAMSUNG-1018)
- U.S. Pat. App. Pub. No. 2009/0019022 to Schallert ("Schallert") (SAMSUNG-1019)
- David Flanagan, O'Reilly & Associates, Inc., "Java in a Nutshell," 1996, ISBN: I-56592-183-6 (SAMSUNG-1020)
- Richard Stevens et al., "UNIX Network Programming Volume 1, Third Edition: The Sockets Networking API," 2003, ISBN: 0-13-141155-1 (SAMSUNG-1021)
- U.S. Pat. App. Pub. No. 2009/0093247 to Srinivasan ("Srinivasan") (SAMSUNG-1022)
- U.S. Pat. App. Pub. No. 2008/0311897 to Segal ("Segal") (SAMSUNG-1023)
- Buxton, B., "Integrating the Periphery and Context: A New Model of Telematics," in *Proceedings of Graphics Interface '95*, in GI'95. 1995 (SAMSUNG-1024)
- Hinckley et al., "Foreground and background interaction with sensor-enhanced mobile devices," *ACM Trans. Comput.-Hum. Interact.*, vol. 12, no. 1, pp. 31–52, Mar. 2005 (SAMSUNG-1025)
- International Publication No. WO 03/100581 to Dive-Reclus ("Dive-Reclus") (SAMSUNG-1026)

31. My analysis and conclusions set forth in this declaration are based on the perspective of a POSITA.

VII. OVERVIEW OF THE ’976 PATENT

A. Specification

32. The ’976 patent is directed to “a wireless end-user device that has wireless wide-area network (WWAN) and wireless local-area network (WLAN) modems.” SAMSUNG-1001, Abstract.

33. In particular, a system “analyzes traffic from [a] network service consuming application,” and “categorize[s] the traffic” based on various criteria, such as “network type, time of day, connection cost, whether home or roaming, network busy state, QoS, and whether the particular service usage activity is in foreground of user interaction or in the background of user interaction.” *Id.*, 100:56-101:39. The system uses one or more policies to “determine an appropriate prioritization for traffic to and/or from the network service consuming application.” *Id.*, 101:47-57. For example, in accordance with one or more policies, the system can selectively (i) “cause[] the network service consuming application ... traffic to be queued in [an] application traffic cache” for transmission over a network (*Id.*, 101:53-102:11), or (ii) “restrict network access of a particular service usage activity” (*Id.*, 102:12-37).

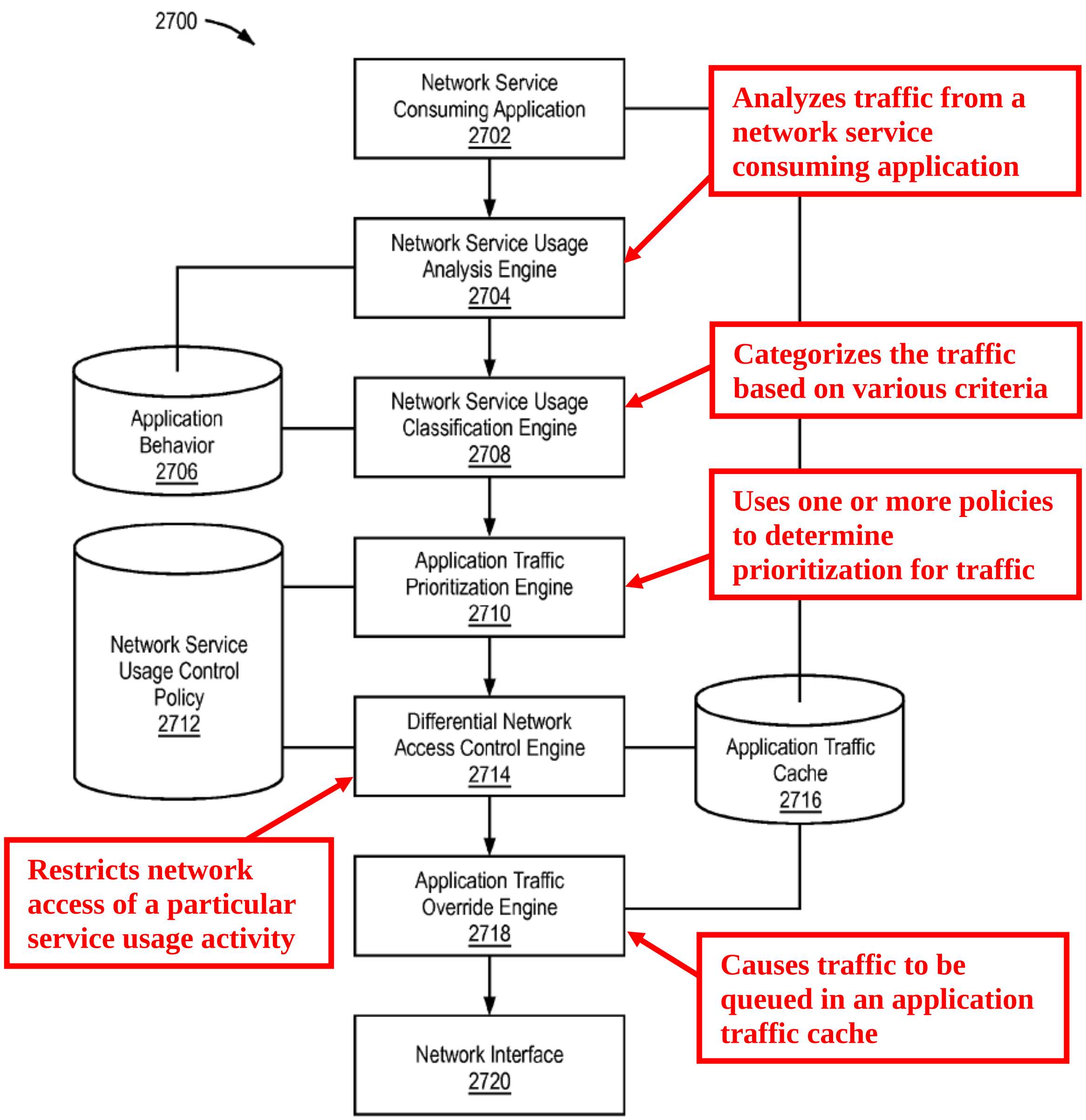


FIG. 27

SAMSUNG-1001, FIG. 27 (annotated)[1]

[1] Annotations to figures throughout are shown in color

B. Claims

34. The table below includes identifiers for the ’976 patent claims and limitations, which are referenced throughout.

Claim	Identifier	Claim Language
1	[1.1]	A wireless end-user device, comprising:
	[1.2]	a wireless wide area network (WWAN) modem to communicate data for Internet service activities between the device and at least one WWAN, when configured for and connected to the WWAN;
	[1.3]	a wireless local area network (WLAN) modem to communicate data for Internet service activities between the device and at least one WLAN, when configured for and connected to the WLAN;
	[1.4]	a device display;
	[1.5]	one or more processors configured to
	[1.6]	classify, for a first end-user application capable of interacting in the device display foreground with a user and capable of at least some Internet service activity when not interacting in the device display foreground with the user, whether or not the first end-user application, when running, is interacting in the device display foreground with the user,
	[1.7]	for a time period when data for Internet service activities is communicated through a WWAN modem connection to the at least one WWAN, apply a first differential traffic control policy to Internet service activity on behalf of the first end-user application, such that Internet service activity on behalf of the first end-user application is disallowed when the one or more processors classify the first end-user application as not interacting in the device display foreground with the user, and
	[1.8(a)]	indicate to the first end-user application, via an

Claim	Identifier	Claim Language
		application program interface (API), one or more network access conditions based on the applied first differential traffic control policy,
	[1.8(b)]	including a first network access condition that indicates the unavailability to the first end-user application, when the first end-user application is classified as not interacting in the device display foreground with the user, of Internet data service that is available via the WWAN modem, and
	[1.8(c)]	a second network access condition that indicates the availability to the first end-user application, when the first end-user application is classified as interacting in the device display foreground with the user, of Internet data service that is available via the WWAN modem.
2	[2]	The wireless end-user device of claim 1, wherein the one or more processors are configured to classify that the first end-user application is not interacting in the device display foreground with the user when the user of the device is not directly interacting with that application or perceiving any benefit from that application.
3	[3]	The wireless end-user device of claim 1, further comprising a user interface to provide the user of the device with information regarding why the first differential traffic control policy is applied to the first end-user application.
4	[4]	The wireless end-user device of claim 1, further comprising a user interface to inform the user of the device when there are options to set, control, override, or modify service usage controls that affect the first differential traffic control policy.
5	[5]	The wireless end-user device of claim 1, wherein the first differential traffic control policy is part of a multimode profile having different policies for different networks.

Claim	Identifier	Claim Language
6	[6]	The wireless end-user device of claim 5, wherein the one or more processors are further configured to select a traffic control policy from the multimode profile based at least in part on the type of network connection currently in use by the device.
7	[7]	The wireless end-user device of claim 6, wherein the one or more processors are further configured to, when the type of network connection is at least one type of WLAN connection, select a traffic control policy from the multimode profile based at least in part on a type of network connection from the WLAN to the Internet.
8	[8.1]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to classify whether a second end-user application is interacting in the device display foreground with the user,
	[8.2]	apply a second differential traffic control policy to Internet service activity on behalf of the second end-user application, and
	[8.3]	indicate to the second end-user application, via the API, one or more network access conditions based on the applied second differential traffic control policy.
9	[9]	The wireless end-user device of claim 1, further comprising a network stack interface integrated with the API.
10	[10]	The wireless end-user device of claim 1, further comprising a networking stack, wherein the one or more processors are further configured to, at an application service interface layer, identify application traffic flows prior to the flows entering the networking stack.
11	[11]	The wireless end-user device of claim 1, wherein the one or more processors apply the first differential traffic control policy to one of but not both of a connection to a roaming WWAN network and a connection to a home WWAN network.

Claim	Identifier	Claim Language
12	[12]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change the application of the first differential traffic control policy based on a power state of the device.
13	[13]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change the application of the first differential traffic control policy based on a device usage state.
14	[14]	The wireless end-user device of claim 1, wherein the one or more processors configured to classify whether or not the first end-user application, when running, in interacting in the device display foreground with a user perform the classification based at least in part on a state of user interface priority for the application.
15	[15]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change the application of the first differential traffic control policy based on power control state changes for one or more of the modems.
16	[16]	The wireless end-user device of claim 1, wherein the one or more processors are configured to associate the first end-user application with the first differential traffic control policy based on an application behavior.
17	[17]	The wireless end-user device of claim 1, wherein the differential traffic control policy defines that applications to which the policy applies can only have WWAN network access events during particular time windows.
18	[18]	The wireless end-user device of claim 1, wherein the one or more processors are further configured to update the first differential traffic control policy based on information received from a network element.
19	[19]	The wireless end-user device of claim 1, further

Claim	Identifier	Claim Language
		comprising an agent to block, modify, remove, or replace, based on the applied differential traffic control policy, user interface messages generated by the first end-user application.
20	[20]	The wireless end-user device of claim 1, wherein the one or more processors configured to apply the first differential traffic control policy to disallow Internet service activity on behalf of the first end-user application perform a disallowance of Internet service activity by intercepting open, connect, and/or write requests by the first end-user application to a network stack.
21	[21]	The wireless end-user device of claim 20, wherein the API responds to an intercepted request by the first end-user application by emulating network messaging.
22	[22]	The wireless end-user device of claim 21, wherein emulating network messaging comprises responding to a network request from the first end-user application by blocking the request from passing to a network stack and returning to the first end-user application a message indicating the network request was not successful.
23	[23]	The wireless end-user device of claim 1, the first differential traffic control policy comprising first and second sub-policies applicable respectively to Internet data service provided using the WWAN modem to connect to a home WWAN and a roaming WWAN, wherein the one or more processors are further configured to apply the first sub-policy when Internet data service is provided through a home WWAN and to apply the second sub-policy when Internet data service is provided through a roaming WWAN.
24	[24]	The wireless end-user device of claim 1, the first differential traffic control policy comprising first, second, and third sub-policies applicable respectively to Internet data service provided using the WWAN modem

Claim	Identifier	Claim Language
		and three different network types from the network types consisting of 2G, 3G, 4G, home, and roaming.
25	[25]	The wireless end-user device of claim 1, wherein the API comprises a network access API.
26	[26]	The wireless end-user device of claim 1, wherein the one or more network access conditions indicated via the API to the first end-user application comprises information on whether a current connected WWAN is a roaming network or a non-roaming network.
27	[27]	The wireless end-user device of claim 1, wherein the API informs the first end-user application when it is allowed to access Internet data service that is available via the WWAN modem.
28	[28]	The wireless end-user device of claim 1, wherein the API informs the first end-user application of one or more network traffic controls that the first end-user application is expected to implement.
29	[29]	The wireless end-user device of claim 1, wherein the API instructs the first end-user particular application to transition to a different state.

C. Prosecution History

35. The Examiner did not issue a prior art rejection in the prosecution of the '976 patent. *See, generally,* SAMSUNG-1002, 337-352. There is no indication in the '976 patent's file history that the Examiner substantively considered several of the prior art applied in this Petition (e.g., Rao, Oestvall, Montemurro, Araujo) prior to allowing the application that issued as the '976 Patent. *Id*. In allowing the claims, the Examiner identified the "closest prior art" as "Cole (USPN 2008/0080457)," "Venkatraman et al (USPN 2008/0034418)," and "Noonan et al

(USPN 2006/0136882)." *Id.*, 6-7. During prosecution, the Examiner did not consider and/or substantively apply any ground of rejection based on Rao, Oestvall, Montemurro, and Araujo. *Id.* As discussed below, these references render obvious the Challenged Claims. While a family member of Cole was considered by the Examiner, its disclosure was not evaluated in combination with Rao and Oestvall, which, as explained in Section XIII below, makes claims 12 and 15 obvious.

VIII. INTERPRETATION OF THE '976 PATENT CLAIMS

36. I have been informed by Counsel and understand that the best indicator of claim meaning is its usage in the context of the patent specification as understood by one of ordinary skill. I further understand that the words of the claims should be given their plain meaning unless that meaning is inconsistent with the patent specification or the patent's history of examination before the Patent Office. Counsel has also informed me, and I understand that, the words of the claims should be interpreted as they would have been interpreted by one of ordinary skill at the time of the invention was made (not today). I have been informed by Counsel that I should use January 28, 2009 as the point in time for claim interpretation purposes.

IX. SUMMARY OF RELEVANT PRIOR ART

A. Rao (U.S. Pat. App. Pub. No. 2006/0039354)

37. Rao is focused on a "remote access architecture" for a system that provides "peer-to-peer communications and remote access connectivity." Rao, Abstract. The system includes clients 105 (instances of computing devices 102) that communicate with each other over a network 104 (and optionally through a gateway 340) and with other types of computing devices, such as servers 102e and server farms 102n. *Id.*, [0086]-[0096].

38. Rao is analogous art to the '976 patent since, like the '976 patent, Rao describes techniques for using policies to regulate network-related activity and/or adjust the operation of applications running on a device. SAMSUNG-1001, 101:47-57. Additionally, Rao describes techniques reasonably pertinent to the problem allegedly solved by the '976 patent. For example, as discussed below, Rao describes techniques for analyzing traffic from an application, categorizing the traffic, and classifying an interaction state of an application based on whether the application is running in the background or the foreground. *Id.*, 100:56-101:39.

39. Figure 1A shows an example of the Rao system:

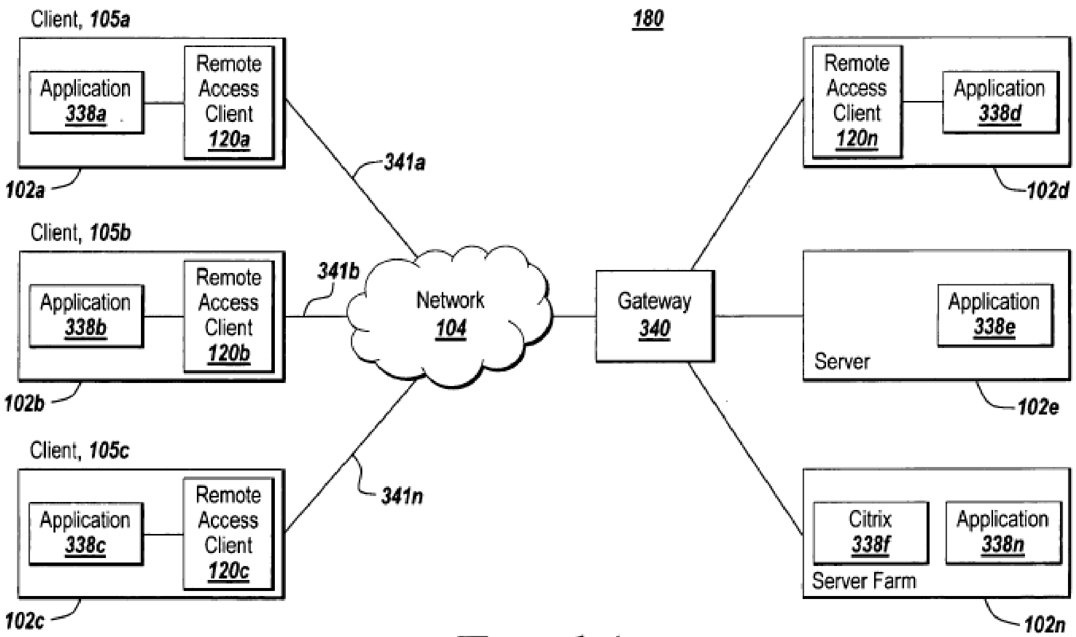


Fig. 1A

Rao addresses inefficient use of network resources when network communications between devices are "processed in the order generated by the activity of a user and applications of the client," which is not "always desirable" since "a network packet generated or received for an application running in the background may be processed ahead of a network packet generated or received for the application running in the foreground." SAMSUNG-1005, [0001]. This results in applications suffering from increased latency and reduced the quality of voice communication. *Id*.

40. Rao contemplates addressing these network inefficiencies through a prioritization scheme that "provide[s] application-aware, client-specific

prioritization of packet traffic." SAMSUNG-1005, [0003]. The prioritization scheme is achieved by augmenting client 105 with a remote access client 120 that interacts with applications 338 and network stack 310. SAMSUNG-1005, [0100].

41. Figure 1C shows an example of a system with a remote access client for routing network packets from client 105 to network 104:

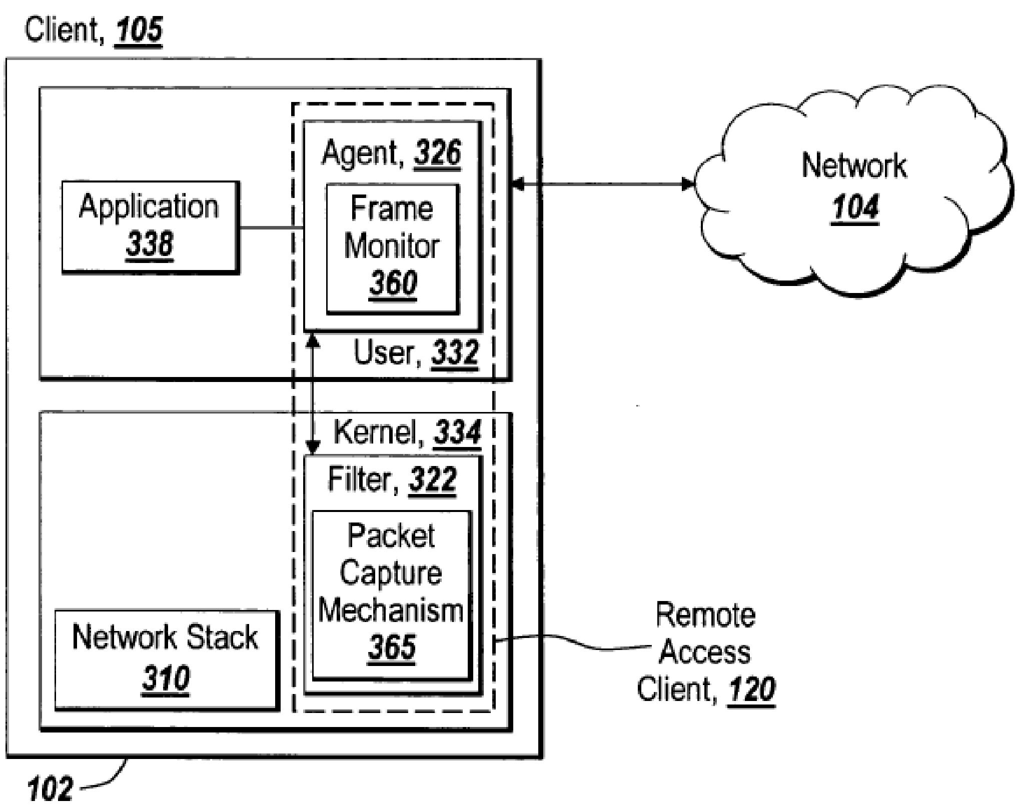


Fig. 1C

42. The remote access client 120 includes a filter 322 that uses a filtering table to determine what action to take against packets," including "ensur[ing] that

unwanted packets are discarded" and "deny[ing] access to particular protocols or to prevent unauthorized access from remote computers by discarding packets to specified destination addresses." SAMSUNG-1005, [0102]. An agent 326 with a frame monitor 360 "include[s] policies and logic for applying a policy to a received packet." *Id.*, [0108]. Frame monitor 360 also "transmit[s] a packet to a gateway 340 responsive to a policy-based determination made by the frame monitor 360." *Id.* Use of policies through remote access client 120 guides efficient use of network resources and thereby enables the Rao system to address the deficiencies identified within Rao's disclosure.

43. The Rao system further enables "intelligent and client centric prioritization of application network communications on a client based on the type and/or priority of an application." *Id.*, [0179], FIG. 5A. To perform this prioritization, the Rao system "appl[ies] a policy to determine a condition of the client 105, or endpoint, at the time of transmission of the packet." SAMSUNG-1005, [0109]. Figure 5A shows an example of a client-side application-aware network communication system:

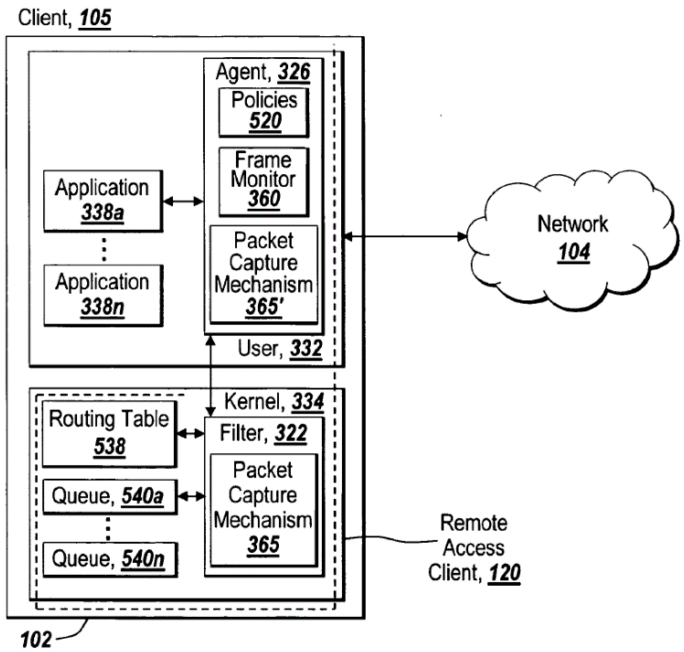


Fig. 5A

44. Rao offers non-limiting disclosure relating to the specification of policies 520 and how its system leverages each of these policies 520 for prioritization. SAMSUNG-1005, [0182] ("policies 520 may be specified by any suitable means and/or mechanisms"). As examples, Rao describes that policies 520 can be specified by "name of the application 338a-338n," "type of application 338a-338n," or "type of one or more protocols used by the applications 338a-338n." SAMSUNG-1005, [0182]. Policies 520 can "define prioritization based on whether an application is running in the foreground or the background of the client 105," "indicate prioritization based on the destination network address, such as host name or IP address, and/or destination port number," and can be "specified

conditionally, such as if one application 338a is running, a second application 338b may have a higher or lower priority." *Id.* Indeed, "[o]ne ordinarily skilled in the art will recognize and appreciate the multitude of ways to define client-side application priorities." *Id.* Policies 520 also can be used to "determine which packets to queue and/or discard." *Id.*, [0207]. Additionally, policies 520 can "apply a priority to network packets of applications 338a-338n in accordance with the prioritization rules specified or indicated by the policies 520." *Id*.

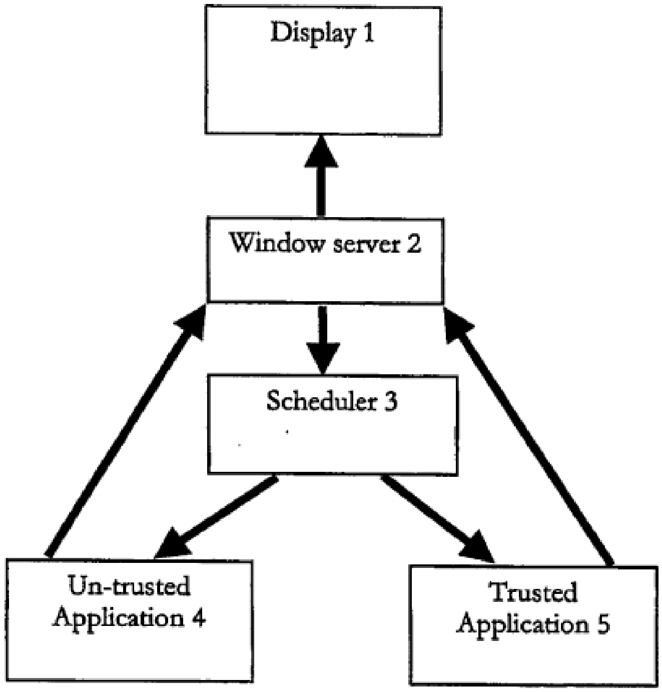
B. Oestvall (U.S. Pat. App. Pub. No. 2007/0038763)

45. Oestvall is focused on techniques to "preserve or conserve resources, such as battery power" on mobile devices. SAMSUNG-1006, [0002]. Oestvall emphasizes that battery consumption is "very important," particularly in devices that "consume high power levels by virtue of connecting to always-on GPRS or 3G cellular networks." *Id.*, [0004]. This problem is "especially acute for multi-tasking devices, i.e., devices with an operating system that can run several applications at the same time." *Id.*, [0007]. This occurs since conventional schedulers used for multitasking may be configured such that "applications will continue to run even when not actually in active use," which results in the applications continuing to "use some system resources, even when residing in the 'background.'" *Id.*, [0006].

46. Oestvall is analogous art to the '976 patent since, like the '976 patent, Oestvall describes techniques for regulating network-related activity and of

applications running on a device. SAMSUNG-1001, 101:47-57. Additionally, Oestvall describes techniques reasonably pertinent to the problem allegedly solved by the ’976 patent. For example, as discussed below, Rao describes techniques for classifying an interaction state of an application based on whether the application is running in the background or the foreground and adjusting an application’s access to device resources based on the classification. *Id.*, 102:12-37.

47. Oestvall addresses these power consumption challenges using techniques that “deny[] system resources and services to background applications that do not meet predefined ‘trust’ or certification criteria,” which it refers to as “untrusted” applications. SAMSUNG-1006, [0010]. Examples of untrusted applications include those that are “not able to access certain predefined protected resources,” from third-party sources and are thereby “loaded from RAM,” or that have not been validated using a “predefined validation or certification process.” *Id.*, [0011]-[0013]. Figure 1 shows an example of the Oestvall system:



48. A window server component 2 determines "if an application is in the background or foreground on display 1." SAMSUNG-1006, [0023]. If the application is an untrusted application 4 and is running in the background, then the window server component 2 "send[s] a control signal to the scheduler 3" that prevents untrusted application 4 from "running, e.g., being given any services or consuming any resources." *Id.* Oestvall offers several non-limiting examples for how scheduler 3 may regulate access to resources by a background untrusted application 4. *Id.* As examples, scheduler 3 may "never allocate any services or resources," or "place any interrupts from [the application] to the back of its queue and never allow them to be executed." *Id.* As another example, scheduler 3 may prevent background untrusted applications 4 from "'polling' for data over a

wireless network," or "from running." *Id.*, [0024]. When an application is in the foreground, then the application may be permitted to "run again—e.g., to be provided with resources and services." *Id.*, [0025].

C. Montemurro (U.S. Pat. App. Pub. No. 2009/0207817)

49. Montemurro is focused on "policy-based routing of communications among two or more modes of wireless communication." SAMSUNG-1007, [0001]. Devices with such connectivity capabilities are "dual or multi-mode devices," with "radio access technologies that provide access to multiple network types," including WLAN, WWAN, and others. *Id.*, [0003]. But "[t]here are costs associated with application access from these different networks" and "[i]t is therefore desirable to have a mechanism that seeks to optimize communications for multi-mode capable devices." *Id.*, [0004].

50. Montemurro is analogous art to the '976 patent since, like the '976 patent, Montemurro describes techniques for enabling network access to different types of wireless networks. SAMSUNG-1001, Abstract. Additionally, Montemurro describes techniques reasonably pertinent to the problem allegedly solved by the '976 patent. For example, as discussed below, Montemurro describes techniques for identifying the types of wireless networks that are available for connection and routing techniques for establishing a connection to the most suitable network. *Id*.

51. Montemurro's mechanism broadly relies on policies to "configure connections and routes." SAMSUNG-1007, [0011]. The configuration is accomplished using a "rules engine" that "evaluates [the] policies on a status change (e.g., network availability, time of day, etc.) to configure a routing table." *Id*. Together with the routing table, the rules engine "provides an appropriate connection to an application for its respective communications." *Id*. Figure 2 (below) shows "policy-based data routing for multi-mode operations of device 102 for communicating with network infrastructure." SAMSUNG-1007, [0024].

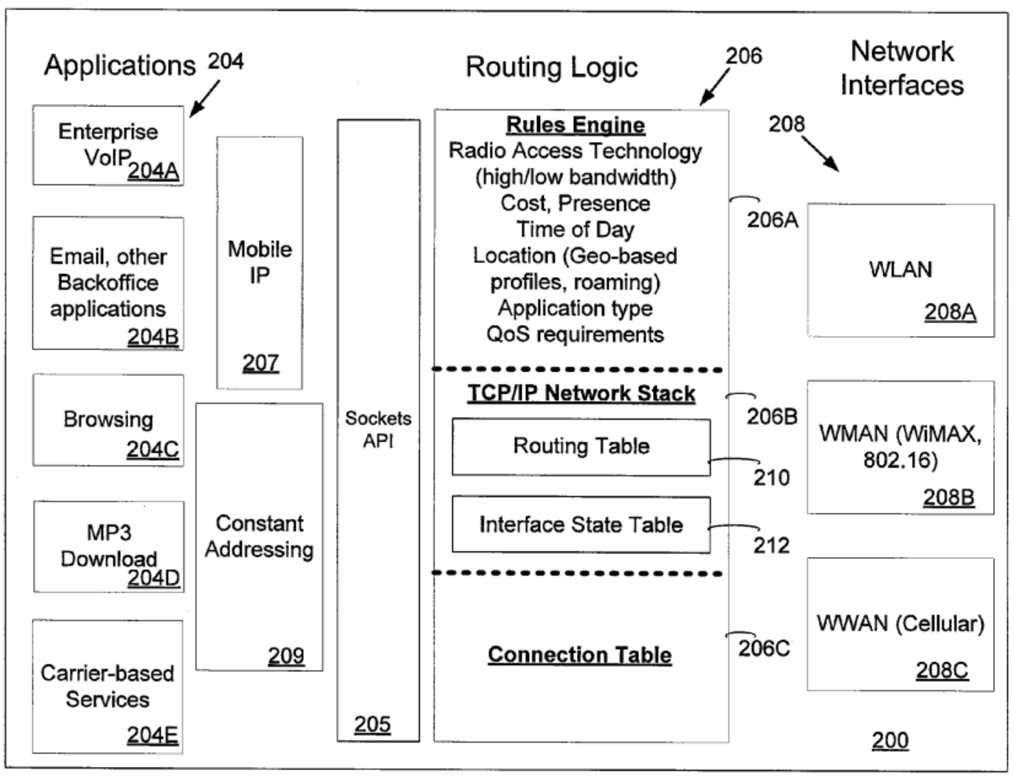


Figure 2

52. Device 102 includes "a plurality of applications 204, routing logic 206, and network interfaces 208." SAMSUNG-1007, [0025]. Routing logic 206

further includes rules engine 206A as a "policy-based mechanism using rules to configure TCP/IP network stack 206B and connection table 206C to coordinate communications for applications 204 using communications interfaces [208]." *Id.*, [0027]. For example, "a rule is a specific policy that is entered in the 'rules engine' for carrying out the policy." *Id.*

53. Network interfaces 208 include "an interface for each of WLAN 208A, WMAN 208B and WWAN 208C network communications," and optionally, "short-range wireless interfaces (e.g., Bluetooth wireless) and interface(s) for wired network communications (e.g., serial interfaces such as USB, RS 232, etc.)." SAMSUNG-1007, [0028]. Rules engine 206A "configures the communication operations with a set of rules/policies" for "various factors such as radio access technology (e.g., for high/low bandwidth properties), cost, presence, time of day, location (e.g., geo-based policies, network roaming), destination IP address, application type, and Quality of Service (QoS) requirements, among others." *Id.*, [0029].

54. Rules engine 206A "configures (i.e. modifies, periodically in response to changes of state and the evaluation of its rules) connection table 207C and routing table 210 to optimize the flow of communications over multiple communications modes (e.g., interfaces 208 and respective networks 104 and 106)." SAMSUNG-1007, [0033]. On a state change, e.g., "time of day,"

"connecting/disconnecting of device 102 with a specific network 104 and 106," rules engine 206A executes and modifies "routing table 210 to ensure that data goes out to the most appropriate network (via respective network interface 208)." *Id.*, [0035]. Rules engine 206A further "determine[s] which interface would be best to service a particular application." *Id.*

D. Araujo (U.S. Pat. App. Pub. No. 2009/0217065)

55. Araujo describes "a power-management policy" for managing a "machine's power usage." SAMSUNG-1011, Abstract. Araujo's policy can be implemented on "[e]lectronic devices," such as "computers, wireless telephones, audio/video equipment, etc.)" *Id.*, [0014]. The policy is applied to "justify [a program] consuming power, depending on what the program is doing." SAMSUNG-1011, [0004]. By implementing this policy, a device can better "use the energy in a way that strikes a balance between providing functionality and maintaining longevity of the charge." *Id.*, [0001].

56. Araujo is analogous art to the '976 patent since, like the '976 patent, Araujo describes techniques for allowing or blocking an application's access to device resources based on a classification of the application. SAMSUNG-1001, 100:56-101:39. Additionally, Araujo describes techniques reasonably pertinent to the problem allegedly solved by the '976 patent. For example, as discussed below, Araujo describes mechanisms to allow or prevent an application from performing

actions based on a power consumption associated with performing those actions. *Id*., 89:8-43.

57. Araujo also teaches that a device can classify programs with respect to various criteria, and selectively provide resources to the programs based on their classifications. SAMSUNG-1011, [0027]. As an example, Araujo describes that programs "may have a status that reflects its worthiness to consume power." *Id*. In particular, a program "may have a 'VIP' status that allows them to consume power in situations where other programs would not be permitted to consume power," where "VIP" typically stands for "very important person," but in this context may be applied to a program in this sense of denoting one program's relative merit or justification to consume energy." *Id*. As Araujo explains, "[w]hether a program is permitted to consume power could be based on a finding as to whether the program's status justifies the consumption of power under the circumstances that are present." *Id*.

58. Araujo teaches that the device can provide resources to the applications differently, based on whether the applications are "worthy" to consume power. SAMSUNG-1011, [0024]. For example, Araujo describes that a program can generate "a request to perform an action using a particular device, such as "a request to send data over a wireless network" using a "wireless network card." *Id*., [0020], [0024].

59. In response, the device can selectively perform various operations with respect to the request, including:

(i) "Allow[ing]" the request if the power management policy "allows the device's power state to be changed," such as powering-on a device that is in an "off state" or send the request to a device that is "already powered on" (SAMSUNG-1011, [0035]; FIG. 3, 302), or

(ii) "Block[ing]" the request if the power management policy "does not allow the device's power state to be changed," either permanently or temporarily, such as by queuing the request, blocking the request, dropping the request, delaying the request, and/or referring the request to another device (*Id.*, [0035], [0050]; FIG. 4, 406).

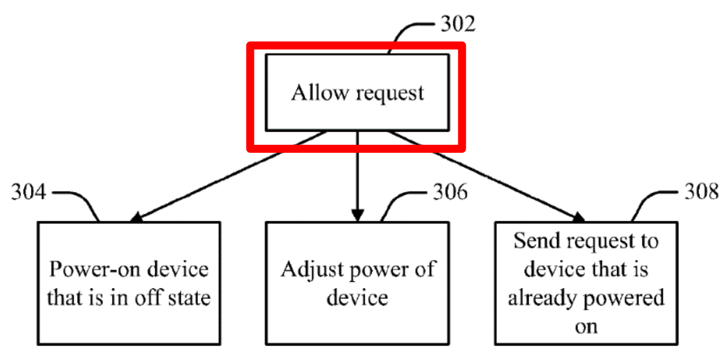


FIG. 3

SAMSUNG-1011, FIG. 3 (annotated)

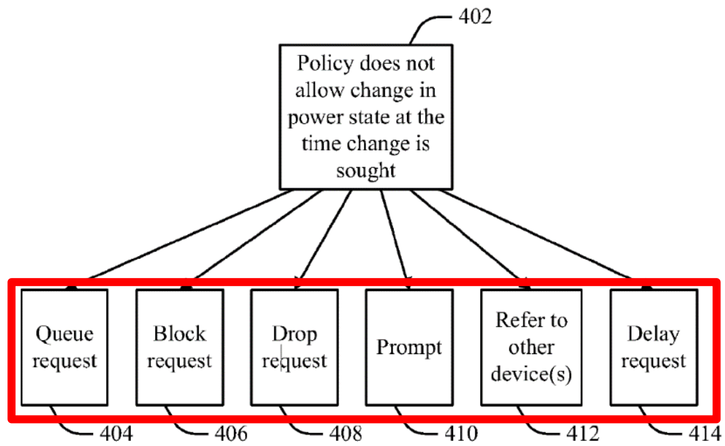


FIG. 4

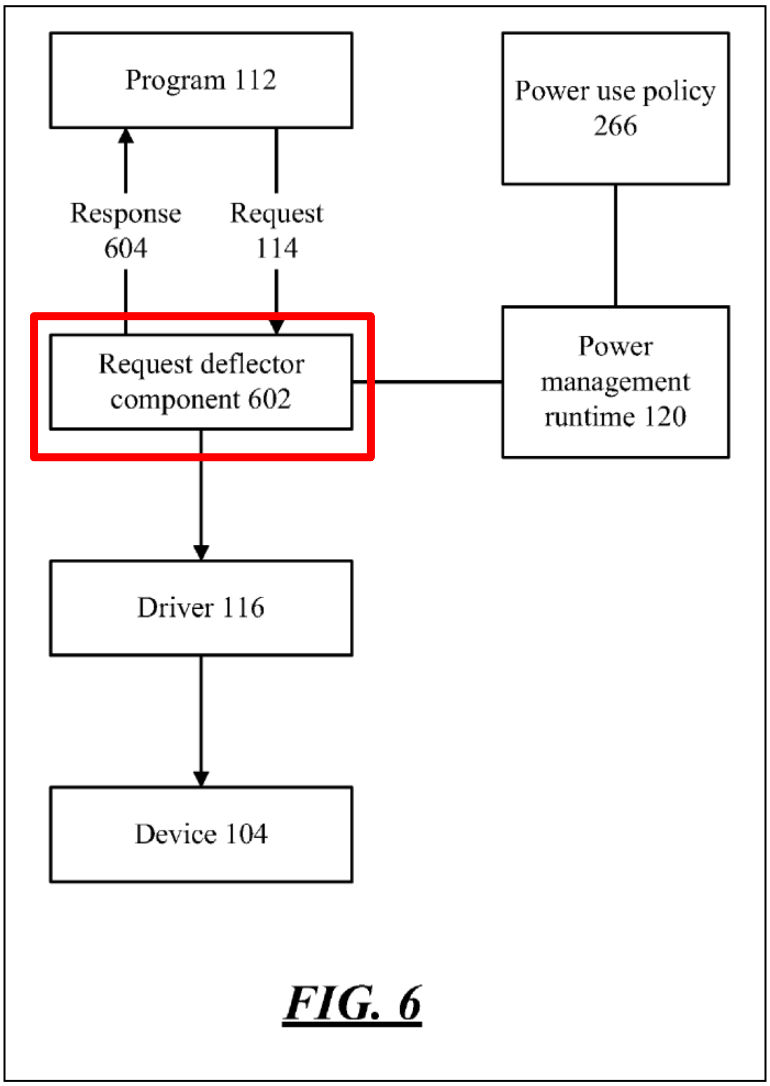
SAMSUNG-1011, FIG. 4 (annotated)

60. Specifically, Araujo describes selectively allowing or blocking a request using a “request deflector component” that is “interposed” between a “program” and a “driver” of a “device,” and configured to “intercept[] requests and respond[] to the requests based on power management considerations before the request reach a device driver.” SAMSUNG-1011, [0024], [0050]. As Araujo explains:

> Request deflector component 602 is a component that is interposed between program 112 and driver 116. Request deflector component receives requests before the requests are conveyed to drivers. When request deflector component 602 detects that a request (such as request 114) has been made, it interacts with power management runtime 120 to determine what the ambient policy (e.g., power use policy 266) says about whether the request may be carried out at the expense of power

use. **<u>If power management runtime 120 determines that request 114 may be carried out under the power policy, then request deflector component 602 passes the request along to driver 116. Otherwise, request deflector component may permanently or temporarily deflect the request from reaching driver 116</u>**."

Id. (emphasis added).



SAMSUNG-1011, FIG. 6 (annotated)

61. Araujo describes that the "request deflector component" can be used to mediate a program's request to any of several different types of devices. As one example, Araujo describes that "device 104 may be machine 102's wireless network card, and request 114 may be a request [by the program 112] to send data over a wireless network." *Id.*, [0020]. Based on the program 112's "worthiness" to consume power (*e.g.*, whether the program is "VIP" or "non-VIP"), the request deflector 602 can selectively:

(i) Power on the network card "in order to allow the device to service the request" (*Id.*, [0037]; FIG. 3, 304),

(ii) Use the "already-powered" network card "to service the program's request" (*Id.*, [0037]; FIG. 3, 308), and/or

(iii) "Block the request" for usage of the network card (*Id.*, [0040]; FIG. 4, 406).

That is, Araujo's device selectively allows a program's request when it deems that the program is sufficiently important to consume resources (e.g., "worthy" programs, such as "VIP" programs), while selectively denying the program's request when it deems that the program is not sufficiently important to consume resources (e.g., programs that are not "worthy," such as "non-VIP programs).

X. [GROUND 1A] - RAO AND OESTVAL MAKES CLAIMS 1-4, 8-10, 13, 14, 16, 18-20, 25, 27-29 OBVIOUS

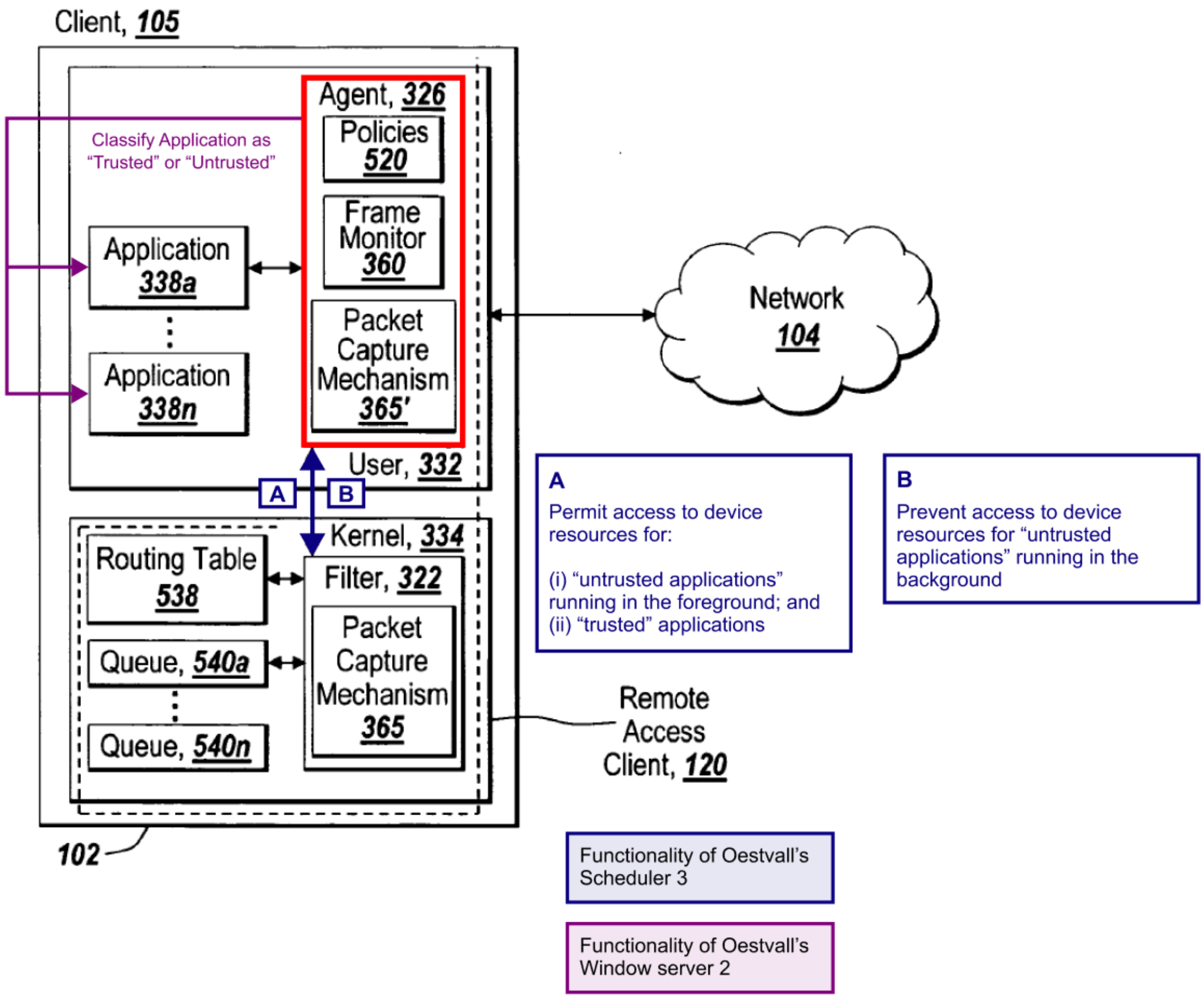
A. Combination of Rao and Oestvall

62. As described above, Rao describes applying policies to prioritize transmission of certain higher-priority network packets over other lower-priority network packets. SAMSUNG-1005, [0179]-[0195], FIG. 5A. While Rao teaches that such prioritization techniques would have improved the efficient utilization of network resources, a POSITA would have further understood that the prioritization techniques may have implications not specifically addressed within Rao's disclosure. For instance, by the Critical Date, a POSITA would have recognized that Rao's prioritization techniques reduces congestion and improves packet throughput. *Id.*; SAMSUNG-1005, [0195]. But Rao does not account for application states in its prioritization techniques, and by the Critical Date, a POSITA would have understood that application states similarly impact the problems addressed in Rao, such as network usage efficiency. A POSITA looking to implement Rao would have been motivated to look to solutions to address improve Rao's packet-based prioritization techniques. *Id.*

63. In seeking solutions, a POSITA would have identified Oestvall, which, like Rao, is broadly focused on achieving efficiencies associated with mobile device operation. SAMSUNG-1006, [0002]. Oestvall further offers techniques to "preserve[] system resources by denying system resources and

services" to certain applications. SAMSUNG-1006, [0010]. A POSITA would have found obvious integration of Oestvall's resource conservation techniques into the Rao system to promote more efficient peer-to-peer communications and network access connectivity that also reduces power consumption on a mobile device. As explained below, the resulting Rao-Oestvall device would have performed various types of prioritizations regulating access to device resources by applications, such as those based on network packet transmission (described in Rao) and others based on the classification of an application (described in Oestvall). Given Oestvall's focus on battery conservation, Rao-Oestvall would have therefore enabled prioritization in a manner that conserves battery power.

64. For example, in the Rao-Oestvall device (shown below), a POSITA would have improved the agent 326 (red) to incorporate functionality associated with Oestvall's window server 2 (purple) and functionality associated with scheduler 3 (blue). SAMSUNG-1006, [0023]. Such a configuration would have enabled an improved agent to classify applications 338a-n (for which packet transmissions are prioritized) as an "trusted" or "untrusted" application. *Id*. The configuration would have also enabled the improved agent to prevent an untrusted application from running or being given access to a service that consumes resources. *Id.* Below is a visual diagram of the Rao-Oestvall combination discussed above.



Rao-Oestvall

65. A POSITA would have found obvious that Rao-Oestvall shown above enables policies that provide various types of prioritizations, consistent with Rao. SAMSUNG-1005, [0182]. This would have improved use of policies in certain network scenarios contemplated in Rao. Policies may be used to prevent network packet transmissions of applications that would have otherwise been prioritized by Rao and contributed to additional power consumption.

66. To implement the functionality discussed above, a POSITA would have also modified Rao's policies 520 to include logic relating to a classification of an application. Such a modification is consistent with Rao, which specifies that the policies already "may be specified by the name of the application 338a-338n and/or the type of application 338a-338n." SAMSUNG-1005, [0182]. Rao describes that policies "define prioritization based on whether an application is running in the foreground or the background of the client 105." *Id.* A POSITA would have found it natural to implement the Rao-Oestvall device such that the policies used by the device indicate information for both packet-based and application-based prioritizations.

67. Finally, configuring Rao's client to leverage Oestvall's teachings would have required only routine programming knowledge well within the skill of a POSITA prior to the earliest effective filing date. Indeed, the change would have amounted to nothing more than the use of a known technique to improve similar devices – in each instance a smart phone equipped with software to regulate device activity based on monitoring user-device interactions – in a similar way, and combining prior art elements according to known methods to yield the predictable results described above.

68. The elements of the resulting Rao-Oestvall system would each perform functions they had been known to perform prior to the combination—

client 105 would perform the same functions to prioritize higher-priority messages over lower-priority messages through the use of policies 520, as taught in Rao, but would leverage functionality offered by Oestvall's window server 2 and scheduler 3 to identify a classification of an application (trusted, untrusted) and the application's interaction state (foreground, background. Accordingly, a POSITA would have naturally expected success when incorporating Oestvall's teachings into the Rao system, as described above.

B. Analysis of Claims 1-4, 8-10, 13, 14, 16, 18-20, 25, 27-29

1. *Claim 1*

[1.1] A wireless end-user device, comprising:

69. Even if the preamble were properly limiting (it is not), Rao-Oestvall discloses it. As discussed in Section XI.A, Rao-Oestvall provides a device representing a type of "***wireless end-user device***." Rao describes "multiple computing devices 102a-102c" (also referred to as "clients 105a-105c)," which connect to a network using one or more network connections. SAMSUNG-1005, [0086]. Client 105 can be "any type and/or form of computing device 102 that can run one or more applications 338," such as a "web browser, web-based client, client-server application, a thin-client computing client." *Id.*, [0088]. Client 105 may also be a "mobile client," such as a "notebook, personal digital assistant (PDA), a smart phone" or "telecommunication device." *Id.*, [0198].

[1.2] a wireless wide area network (WWAN) modem to communicate data for Internet service activities between the device and at least one WWAN, when configured for and connected to the WWAN;

70. The Rao-Oestvall device would have included network connectivity features that Rao describes for device 102 (client 105), thereby rendering this limitation obvious. Device 102 includes network interface 118, which enables connectivity to "Local Area Network (LAN), **Wide Area Network (WAN)** or the Internet through a variety of connections," such as "standard telephone lines, LAN or WAN links," "broadband connections," "wireless connections," or "some combination of any or all of the above." SAMSUNG-1005, [0095], [0125]. Network interface 118 includes "a built-in network adapter, network interface card, PCMCIA network card, card bus network adapter, USB network adapter, modem, or any other device suitable for interfacing the computing device 102 to any type of network capable of communication…" *Id.* Given such non-limiting disclosure, a POSITA would have understood and found obvious to implement network interface 118 to enable multiple types of network connectivity such that network interface 118 includes, among others, a "***wireless wide area network (WWAN) modem***" to permit the Rao-Oestvall device to communicate with network 104 as a WWAN ("***at least one WWAN***") for accessing services associated with a remote access client ("***communicate data for Internet service activities***"). SAMSUNG-1005, [0172], [0198].

71. Network configurations for mobile devices that enabled WLAN and WWAN connectivity and techniques for alternating connectivity between such configurations were conventional by the Critical Date. For example, Cole describes a mobile device 110 that includes one or more "communication interfaces 225," including, for example, "a ***WWAN modem 230***, a WLAN modem 235, a LAN device 240, a WPAN device 245, and a voice band modem 250 (e.g., V90)." SAMSUNG-1009, [0035], FIG. 2. As another example, Montemurro describes that "if both the WLAN and WWAN radios…of [a] device [] **<u>are connected</u>** to their respective networks 104 and 106, there will be a route associated with each network 104 and 106…" *Id.*, [0030].

[1.3] a wireless local area network (WLAN) modem to communicate data for Internet service activities between the device and at least one WLAN, when configured for and connected to the WLAN;

72. As discussed for [1.2], Rao provides non-limiting disclosure relating to network connectivity features provided by network interface 118, which would have been included in the Rao-Oestvall device. SAMSUNG-1005, [0095], [0125]. Network interface 118 enables connectivity to "***Local Area Network (LAN)***, Wide Area Network (WAN) or the Internet through a variety of connections," such as "standard telephone lines, LAN or WAN links," "broadband connections," "wireless connections," or "some combination of any or all of the above." SAMSUNG-1005, [0125]. Given such non-limiting disclosure, a POSITA would

have understood and found obvious to implement network interface 118 to enable multiple types of network connectivity such that network interface 118 includes, among others, a "***wireless local area network (WLAN) modem***" to permit the Rao-Oestvall device to communicate with network 104 as a wireless LAN ("***at least one WLAN***") for accessing services associated with a remote access client ("***communicate data for Internet service activities***"). Network configurations for mobile devices that enabled WLAN and WWAN connectivity and techniques for alternating connectivity between such configurations were conventional by the Critical Date. *See, e.g.*, SAMSUNG-1007, [0030]; SAMSUNG-1009, [0035], FIG. 2.

[1.4] a device display;

73. The Rao-Oestvall device incorporates hardware elements of Rao's device 102, including a "***display device***" for displaying content and information associated with applications 338. SAMSUNG-1005, [0118]. For example, device 102 includes a "visual display device 124" for displaying information pertinent to use of the device as, for instance, a "personal computer or computer server." *Id.*; *see also id.*, [0122], FIG. 1D. Rao further indicates existence of a display device in device 102 since "agent 326 may provide a configuration mechanism such as a user interface, graphical or otherwise, designed and constructed for configuring or specifying the policies 520." *Id.*, [0183].

[1.5] one or more processors configured to

74. The Rao-Oestvall device incorporates hardware elements of Rao's device 102, including "***one or more processors***" for executing instructions relating to device functionality. SAMSUNG-1005, [0118]. For example, device 102 includes "central processing unit [112],"[2] which may be "any logic circuitry that responds to and processes instructions from the main memory 104." *Id.*, [0119].

[1.6] classify, for a first end-user application capable of interacting in the device display foreground with a user and capable of at least some Internet service activity when not interacting in the device display foreground with the user, whether or not the first end-user application, when running, is interacting in the device display foreground with the user,

75. The Rao-Oestvall device incorporates software elements of Rao's device 102, including applications 338 that represent examples of the "***first end-user application***." SAMSUNG-1005, [0179]. Applications 338 are capable of "***interacting in the device display foreground***" given examples of the applications in Rao, such as a "web browser," "web-based client," "client-server application," and "thin-client computing client." *Id.*, [0088]. A POSITA would have understood that a web browser interacts in the device display foreground since its use involves

---

[2] Figure 1D of Rao depicts a "CPU 112," which is described in paragraphs [0118] and [0119] as "central processing unit 102." For consistency, this Petition references the disclosed element as central processing unit (CPU) 112.

a user interacting with one or more browser interfaces. Moreover, because Rao's policies 520 "define prioritization based on whether an application is running in the foreground or the background of the client 105," applications that are prioritized using policies 520 (e.g., applications 338) are thereby capable of operating in either the foreground or background. SAMSUNG-1005, [0182].

76. In the Rao-Oestvall device, applications 338 are also capable of ***"at least some Internet service activity when not interacting in the device display foreground with the user***." Rao recognizes that "an application running in the background may be processed ahead of a network packet generated or received for [an] application running in the foreground," indicating that application 338 running in the background is similarly capable of network activity. SAMSUNG-1005, [0003]. A POSITA would have understood that applications not running in the foreground (e.g., running in the background) may still be capable of Internet activity. SAMSUNG-1005, [0004]. Indeed, Rao's contemplated "application-aware prioritization of client-side network communications" is premised upon this understanding—that applications not running in the foreground are capable of network activity—since, without it, the problem that Rao discusses in offering its solution is rendered obsolete. *Id.* Rao describes embodiments in which policy 520 "define[s] prioritization based on whether an application is running in the foreground or the background of the client 105." SAMSUNG-1006, [0182]. This

illustrates the existence of at least some scenarios in which an application is not running in the foreground and yet still capable of network transmissions that necessitate prioritization using the policies 520. SAMSUNG-1005, [0182].

77. The Rao-Oestvall device would have also been capable of "***classifying***," for application 338, "***whether or not [the application 338], when running, is interacting in the device display foreground with the user***." As discussed above, because policies 520 define prioritization based on an application's interaction state when running (foreground, background), a POSITA would have understood and found obvious that evaluation of policies 520 by the Rao-Oestvall device involves the type of classification recited by this limitation. Specifically, remote access client 120 (which would have run on the Rao-Oestvall device) "determine[s] whether the application 338a-338n associated with [a] network packet is running in the foreground or the background." SAMSUNG-1005, [0188]. This determination/classification further involves "determin[ing] any priorities, such as process[ing] task priority, assigned to the application 338a-338n by the operating system" of the device. *Id.*

[1.7] for a time period when data for Internet service activities is communicated through a WWAN modem connection to the at least one WWAN, apply a first differential traffic control policy to Internet service activity on behalf

of the first end-user application, such that Internet service activity on behalf of the first end-user application is disallowed

78. Rao-Oestvall would have applied policies (including the "***first differential traffic control policy***") that "define prioritization based on whether an application is running in the foreground or the background of the client 105." SAMSUNG-1005, [0182]. As discussed for [1.6], this classification (foreground, background) is used to apply policies 520 to adjust network transmissions of application 338a. The classification involves "***apply[ing] [the policy 520] to Internet service activity on behalf of [the application 338]***." SAMSUNG-1005, [0003], [0004], [0182], [0188].

79. A POSITA would have found it obvious to configure policy use by the Rao-Oestvall device to increase device efficiency in scenarios where device operation increases battery consumption, such a time period when the device is engaged in network activity over a WWAN network. For example, in Oestvall, "battery conservation in battery operated computing devices is very important, particularly in devices such as smartphones that consume high power levels by virtue of connecting to always-on GPRS or 3G cellular networks." SAMSUNG-1006, [0004]. Given this disclosure, a POSITA would have found it advantageous to implement Rao-Oestvall to apply policies 520 to regulate application activity ("***apply [the policy 520] to Internet service activity on behalf of [the application***

338]”) to reduce battery consumption during time period when its device is connected to “always-on GPRS or 3G cellular networks” (“***a time period when data for Internet service activities is communicated through a WWAN modem connection to the at least one WWAN***”). For example, in at least some scenarios where the Rao-Oestvall device is communicating over a WWAN network, the Rao-Oestvall device would have leveraged Rao’s technique to intercept lower-priority network packets, by leveraging Oestvall’s technique of denying access to services or resource, each of which would have reduced battery consumption.

80. The plain meaning of this limitation does not mean any mobile device configuration in which policy application exclusively occurs when Internet service activities of a mobile device is communicated through a WWAN mode. As explained above, the limitation may be met by any mobile device configuration in which policy application occurs on a mobile device configured to communicate over either a WWAN or WLAN. The Rao-Oestvall device is configured communicate over either a WWAN or WLAN, and has functionality to apply policies in either network scenario, which makes this limitation obvious.

81. Rao also offers broader disclosure of using policy 520 to enable application-aware prioritization. This suggests that policy 520 is applied “***when***” application 338 is classified as not running in the foreground. This interpretation is consistent with Rao’s broader disclosures that policies 520 “specify[] client-side

prioritization of network communications related to applications 338a-338n" (SAMSUNG-1005, [0182]) and its motivation to address a scenario in which "a network packet generated or received for an application running in the background [is] processed ahead of a network packet generated or received for the application running in the foreground" (*id.*, [0003]). Based on these two disclosures, a POSITA would have found obvious that the evaluation of polices by the Rao-Oestvall device to prioritize network transmissions of an application given its interaction state to satisfy any temporal requirement between the use of a policy and classification of an interaction state of an application recited by this limitation.

82. Rao and Oestvall also each disclose techniques for regulating activity of an application based on one or more classifications of the application. Rao-Oestvall renders obvious that applying a policy to prioritize network transmissions of application 338 results in "***Internet service activity on behalf of the [application 338]***" being "***disallowed***" in various ways. For example, a POSITA would have understood and found obvious that the Rao-Oestvall device would have been configured to implement Rao's technique of intercepting network packets of an application based on the application's prioritization. If an application is classified as running in the background, network packets of that application would be stored in a queue behind other application(s) with a higher prioritization, resulting in temporary disallowance of network packet transmission. SAMSUNG-

1005, [0038], [0102]. In this scenario, interception of network packets of the application by the Rao-Oestvall device would have resulted in Internet network service activity associated with intercepted network packets being presently "***disallowed***" until and so long as the device is instead focused on handling "one or more network packets ahead of at least one network packet in the queue" associated with the application. SAMSUNG-1005, [0038], [0046].

83. As another example, a POSITA would have understood and found obvious that the Rao-Oestvall device would have been configured to implement Oestvall's techniques of preventing an untrusted application running in the background from "being given any services or consuming any resources." SAMSUNG-1006, Abstract. As discussed in Section XI.A, this would have been accomplished using an Oestvall-like scheduler in the Rao-Oestvall device based on a classification of application 338 and a determination by an Oestvall-like window server component that determines if the application is running in the foreground or background. SAMSUNG-1006, [0023]. In a scenario where application 338 is an untrusted application presently in the background, the Oestvall-like scheduler would "prevent[] the [application 338] from running," e.g., "operate so as to never allocate any services or resources to the [application 338]." *Id.* Because Internet network service activity is a type of service or resource service, in this scenario, the prevention of access to resources and services for the application 338 by Rao-

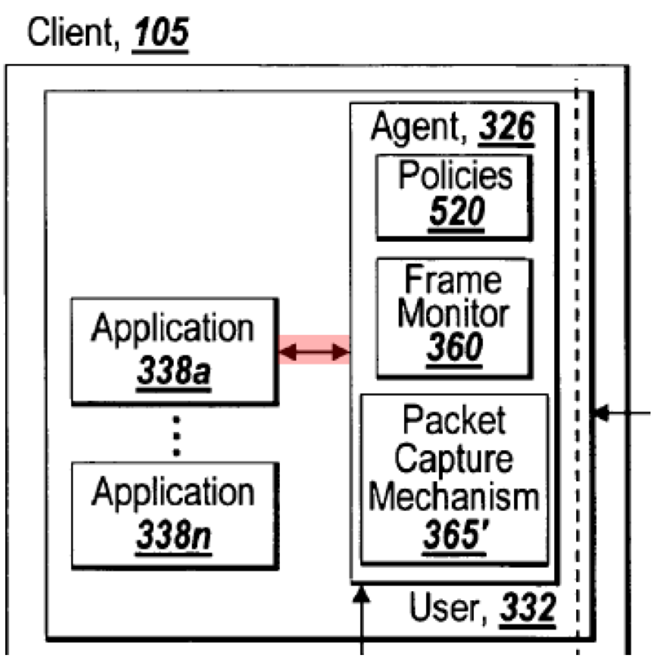
Oestvall device would have resulted in the Internet network service activity associated with application 338 being "***disallowed***" as long as the application 338 remains in the background (based on its classification as an untrusted application).

[1.8(a)] indicate to the first end-user application, via an application program interface (API), one or more network access conditions based on the applied first differential traffic control policy,

84. As discussed in Section XI.A, a POSITA would have configured Rao-Oestvall to perform various types of prioritizations, such as those based on network packet transmission (described in Rao) and others based on the classification of an application (described in Oestvall). SAMSUNG-1005, [0003], [0004], [0182], [0188]; SAMSUNG-1006, [0002], [0023]. As discussed below, the Rao-Oestvall device would have enabled a configuration that regulates an application's access to system resources (e.g., resources for accessing a network), rendering the requirements of this limitation obvious.

85. Rao-Oestvall includes an improved version of Rao's agent 326 that regulates applications by applying a policy ("***applied first differential traffic control policy***"). For example, in Oestvall, an applied policy specifies a condition that "prevents [an] untrusted application 4 from running," including accessing device network resources ("***one or more network access conditions***"). SAMSUNG-1006, [0023]. Since this condition impacts normal operation of the application, a POSITA would have understood and found it obvious that Rao-

Oestvall provides an indication to the application. For example, Rao's Figure 5A (annotated below) shows a bi-directional arrow (red), indicating that, in some instances, agent 326 provides communications to applications 338a-n. Agent 326 includes packet capture mechanism 365, which may use any hooking application programming interface (API) to intercept, hook, or otherwise **obtain inbound and/or outbound packets of the client 105, such as the network traffic associated with application 338**." Rao, [0110].



Oestvall similarly contemplates embodiments in which a policy decision is communicated to an applications, since the application "**maybe requested** (but not prevented) to stop running if in background)." SAMSUNG-1006, [0015], [0023] (describing alternatives for regulating an application). Based on these disclosures, when Rao-Oestvall prevents an application running in the background from

accessing device resources (including device network resources), a POSITA would have found it obvious that the application receives an indication relating to prevention ("***indicate to the first end-user application…one or more network access conditions based on the applied first differential traffic control policy***"). *Id*., [0023].

86. A POSITA would have also found it obvious to implement policy evaluation in Rao-Oestvall using one of several well-known techniques that provide indications to applications relating to policy evaluation. As one example, in Araujo (SAMSUNG-1011), "if [a] power state change is not allowable under [a] policy," the device can "block the request" and "notif[y] [the program] that the request will not be processed." SAMSUNG-1011, [0038], [0041]. As discussed in Section XII, a POSITA would have found it obvious to combine Rao, Oestvall, and Araujo to address features described in claims 12, 15, 21, and 22. As another example, Oestvall incorporates by reference Dive-Reclus (SAMSUNG-1026), which teaches using permissions to regulate API calls (e.g., granting, blocking) made by applications in accessing a network. SAMSUNG-1006, [0020]; SAMSUNG-1026, 16:23-17:28, 20. In this example, a POSITA would have found it obvious that a permission decision for an API call (e.g., granting, blocking) by an application involves providing an indication to the application regarding the permission decision. *Id*.

87. Based on Rao's disclosure of API usage, the improved agent in Rao-Oestvall would have leveraged several types of application programming interfaces (APIs) in regulating applications. Rao contemplates using several types of APIs, including an IOCTL API for interfacing with device drivers (SAMSUNG-1005, [0106], [0190]) and a hooking API for intercepting and/or hooking network traffic of applications (*id.*, [0166]). Rao also offers broader disclosure of leveraging any suitable "means" or "mechanism" to implement functionality relating to prioritization (e.g., interception). *Id.*, [0106]. Likewise, Oestvall incorporates by reference Dive-Reclus, which teaches permissions regulating network access by a third-party application that uses an API call, and a POSITA would have found obvious that a permission decision (e.g., grant, deny) is communicated to the third-party application through a corresponding API. SAMSUNG-1006, [0020]; SAMSUNG-1026, 16:23-17:28, 20. Given these disclosures, a POSITA would have understood and found obvious that APIs leveraged by the improved agent of Rao-Oestvall include those described in Rao and Oesvall, as well as conventional APIs known by the Critical Date to support application operations in mobile devices.

88. One example is Java sockets API through which an application communicates data over a network. SAMSUNG-1020, 3-4. Rao describes that its device can run the Java operating system, and thus, a POSITA would have

understood and found obvious that in some implementations of the Rao-Oestvall device, applications running on the device would access the network using the Java sockets API. *Id.*; SAMSUNG-1005, [0088], [0128]. In such implementations, when a network access condition is used to prevent an application from accessing the network, a POSITA would have understood and found obvious that the application would have received an indication, via the Java sockets API, of the network access condition.

89. Finally, use of APIs to provide indications to application were well-known by the Critical Date. For example, Schallert describes providing an "API" to "allow[] [a] computer program to execute queries and integrate the results of these queries into the computer program's internal system." SAMSUNG-1019, Abstract. As another example, a conference publication by Flinn et al. described an "API" that "offers both blocking and event-based interfaces…" SAMSUNG-1016, 1. Flinn further indicates existence of "API features to the normal socket interface[,]" including application regulation mechanisms, such as "block[ing] [a] message until the network is available, with an optional timeout," which is "more useful to threaded applications." *Id.*, 3.

[1.8(b)] including a first network access condition that indicates the unavailability to the first end-user application, when the first end-user application is classified as not interacting in the device display foreground

with the user, of Internet data service that is available via the WWAN modem, and

90. As discussed for [1.8(a)], a POSITA would have configured Rao-Oestvall to perform various types of prioritizations, such as those based on network packet transmission (described in Rao) and others based on the classification of an application (described in Oestvall). SAMSUNG-1005, [0003], [0004], [0182], [0188]; SAMSUNG-1006, [0002], [0023]. A POSITA would have found obvious that, in a first scenario involving Rao-Oestvall, an application is classified as an untrusted application and is presently running as a background process. In this scenario, the Rao-Oestvall device would have applied a policy that in effect prevents the application from obtaining access to device resources (including network resources). Applying the policy results in a change in application function. The policy includes a condition ("***first network access condition***") that prevents the application from accessing device resources ("***unavailability to the first end-user application***") running in the background ("***when…not interacting in the device display foreground with the user***"). A POSITA would have understood Oestvall's non-limiting reference to an application "being given any services or consuming <u>any</u> resources" to include network connectivity resources, and thus, found obvious that evaluation of the policy in the first scenario to be pertinent to

"***Internet data service that is available via the WWAN modem***." SAMSUNG-1006, [0023].

91. Additionally, Rao-Oestvall would have provided regulations relating to network access. As discussed for [1.8(a)], Oestvall references permissions regulating network access by a third-party application that uses an API call, and POSITA would have found obvious that where network access is denied, the denial decision is communicated to the third-party application through a corresponding API. SAMSUNG-1006, [0020]; SAMSUNG-1026, 16:23-17:28, 20.

[1.8(c)] a second network access condition that indicates the availability to the first end-user application, when the first end-user application is classified as interacting in the device display foreground with the user, of Internet data service that is available via the WWAN modem.

92. As discussed for [1.8(a)], a POSITA would have configured Rao-Oestvall to perform various types of prioritizations, such as those based on network packet transmission (described in Rao) and others based on the classification of an application (described in Oestvall). SAMSUNG-1005, [0003], [0004], [0182], [0188]; SAMSUNG-1006, [0002], [0023]. A POSITA would have found obvious that, in a second scenario involving Rao-Oestvall, an application is classified as an untrusted application and is presently running as a foreground process. In this scenario, the Rao-Oestvall device would have applied a policy that permits the application to access device resources (including network resources). Applying the

policy results in a change in application function. The policy includes a condition ("***second network access condition***") that permits the application to access device resources ("***available to the first end-user application***") when running in the foreground ("***when…interacting in the device display foreground with the user***"). A POSITA would have understood Oestvall's non-limiting reference to an application "being given <u>any</u> services or consuming <u>any</u> resources" to include network connectivity resources, and thus, found obvious that evaluation of the policy in the first scenario to be pertinent to "***Internet data service that is available via the WWAN modem***." SAMSUNG-1006, [0023] (emphasis added).

93. Additionally, Rao-Oestvall would have provided regulations relating to network access. As discussed for [1.8(a)], Oestvall references permissions regulating network access by a third-party application that uses an API call, and POSITA would have found obvious that where network access is granted, the grant decision is communicated to the third-party application through a corresponding API. SAMSUNG-1006, [0020]; SAMSUNG-1026, 16:23-17:28, 20.

2. ***Claim 2***

[2] The wireless end-user device of claim 1, wherein the one or more processors are configured to classify that the first end-user application is not interacting in the device display foreground with the user when the

user of the device is not directly interacting with that application or perceiving any benefit from that application.

94. As discussed for [1.6] and [1.7], the Rao-Oestvall device would have incorporated the functionality to detect whether an application is presently running in the background ("***is not interacting in the device display foreground with the user***"). From Rao, because policies "define prioritization based on whether an application is running in the foreground or the background of the client 105[,]" Rao's disclosure presumes existence of the capability to detect when an application is not in the foreground. SAMSUNG-1005, [0182], [0188], [0189]. Rao attributes an application "in the foreground" as one that is "currently in active use by the user," which would have led a POSITA to recognize that an application in the background is one that is not currently in active use by the user ("***when the user of the device is not directly interacting with that application or perceiving any benefit from that application***"). SAMSUNG-1005, [0003]. A POSITA would have known that "active use" indicates user interaction, because the only "active" possible participation by the user in the application would be to manipulate the controls on the user interface, e.g., pushing buttons, entering text, etc.

95. Oestvall offers similar disclosure regarding regulating application operation based on whether an application is running in the foreground or the background. SAMSUNG-1006, [0021]-[0023]. A POSITA would have found

obvious that Rao's differentiated use of "foreground" and "background" throughout its disclosure as indicating that examples of applications in the background are those where the user is not presently interacting with the application through a user interface.

96. In addition, techniques for adapting the prioritization for an application or otherwise impacts its operation based on the application's direct user interaction were well-known by the Critical Date. For example, Singh teaches that "when a user interacts with a window, the window becomes the highest priority window." SAMSUNG-1008, 9:33-35. A POSITA would have understood and found obvious that, in response to user interaction, a processor makes an application's window the highest priority (as described by Singh), and, since that application's window is displayed with highest priority, is therefore classifying the application as high priority according to the user interaction. *Id*. Here again, the application with the highest priority is the one with focus, which is what the user is interacting with. Because it is the application the user is paying immediate attention to, it is natural and appropriate for it to have priority over others.

97. As another example, Freund (SAMSUNG-1010) teaches "monitoring of time spent by an employee for 'actively' interacting with the Internet," and notes that "[a]ctive use occurs when a user directly interacts with an Internet application (e.g., Web browser) while that application accesses the Internet."

SAMSUNG-1010, 10:16-24. A POSITA would have known that directly interacting with a Web browser requires the Web browser to be in the UI foreground because user interfaces must be in the foreground to receive input. Freund further explains that "[a] given application itself can be examined for determining whether it is 'active' by determining whether the application receives 'focus' and/or receives user input (e.g., mouse clicks or key strokes)." SAMSUNG-1010, 10:40-44. A POSITA would have known the mouse clicks and key strokes are instances of direct interaction with an application. Freund differentiates such mouse or keyboard use from "background use which occurs when an application or process executing in the background (i.e., does not have "focus") accesses the Internet, such as a mail client which intermittently polls an Internet-based mail server." *Id.*, 10:20:24. In this way, Freund teaches classifying whether an application is executing in the background or foreground. *Id.* Freund teaches classifying that the first end-user application is interacting with the user in the user interface foreground when the user of the device is directly interacting with that application. *Id.*, 10:40-44.

3. ***Claim 3***

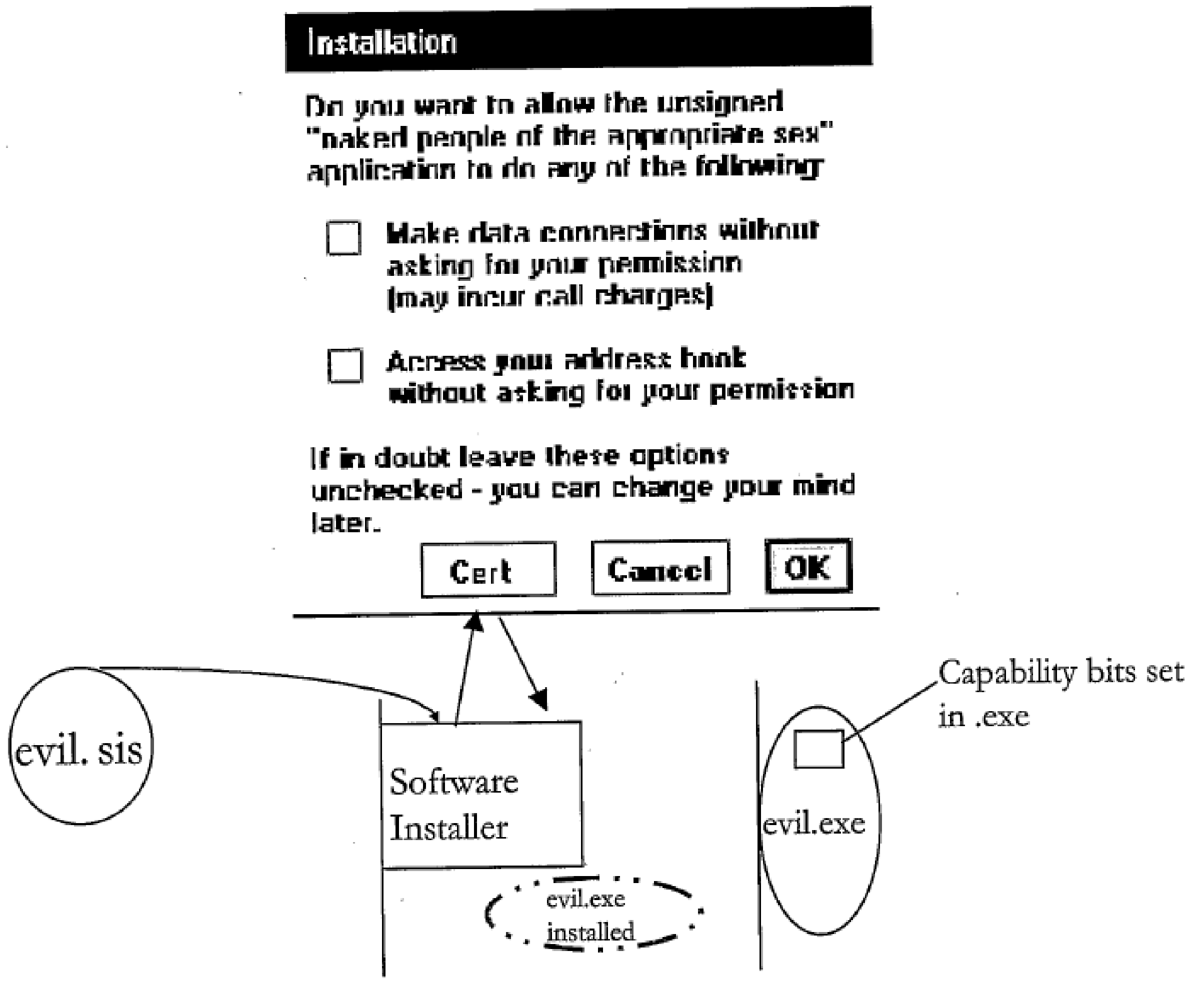
[3] The wireless end-user device of claim 1, further comprising a user interface to provide the user of the device with information regarding why

the first differential traffic control policy is applied to the first end-user application.

98. Rao-Oestvall would have incorporated the functionality to output a user interface relating to various aspects of policies used for prioritization ("***user interface to provide the user of the device with information regarding why the first differential traffic control policy is applied to the first end-user application***"). From Rao, "agent 326 may provide a configuration mechanism such as a user interface, graphical or otherwise, design and constructed for configuring or specifying the policies 520." SAMSUNG-1005, [0183]. Based on this disclosure, POSITA would have found it obvious to configure the agent 326 in the Rao-Oestvall device to similarly provide a user interface to provide information regarding various aspects of applying policies for prioritization, which would include information regarding why the first differential traffic control policy is applied to the first end-user application.

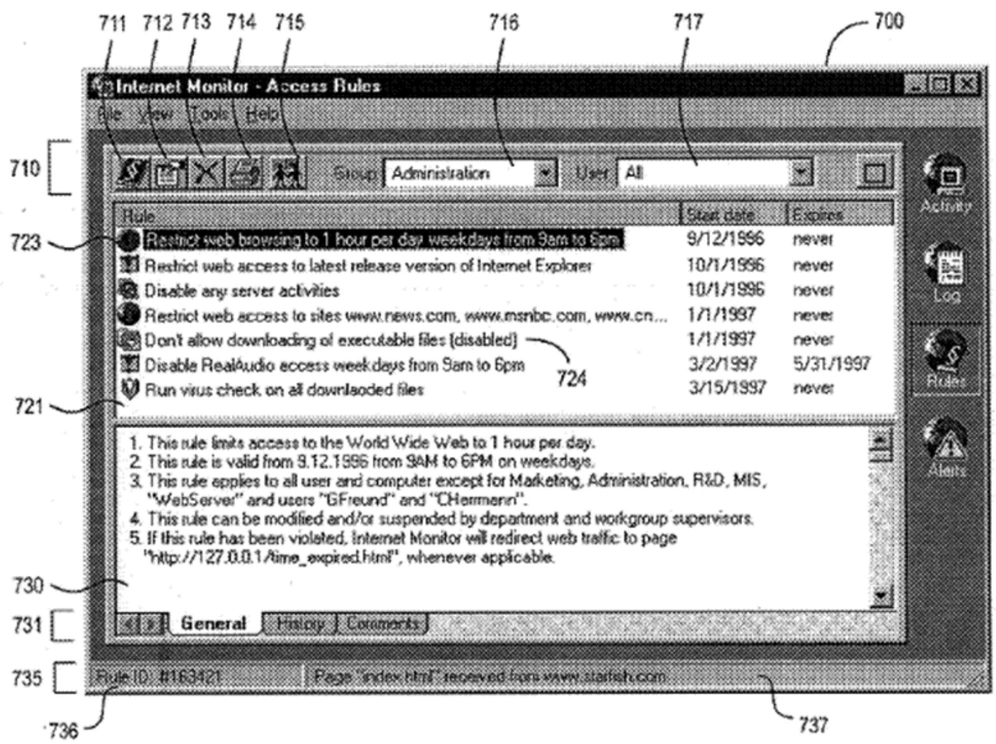
99. As discussed for [1.8(a)], Oestvall incorporates by reference Dive-Reclus, which describes blocking an "unsigned" application and provides an interface requesting a user to confirmation whether the application should be blocked. SAMSUNG-1026, 19:17-25, FIG. 2. As shown in Figure 2 (below), a user interface provides a user with information relating to whether an unsigned application should be granted network access without permission by the user.

Figure 2



SAMSUNG-1026, FIG. 2

100. User interfaces for providing information regarding policy evaluation were well-known before the Critical Date. For example, Freund (SAMSUNG-1010) includes Figure 7A illustrating an example user interface:



SAMSUNG-1010, FIG. 7A

101. Freund further states, "FIGS. 7A-K illustrate a preferred user interface or 'wizard' dialogs for configuring rules, and "in FIG. 7A, a preferred interface 700 provides a 'view' of rules governing operation of the Internet access monitor, displaying all of the rules which are available for a current configuration." SAMSUNG-1010, 24:16-20. Freund further teaches that the policies (rules) can be associated with applications using the "wizard dialog 740 [that] asks the user what kind or type of new rule should be created." *Id.*, 25:1-3, FIGS. 7A-K. Freund further teaches that "any given rule is a combination of access rights granted on the basis of available applications, permitted time limits, permitted user activities,

permitted protocols, and the like." *Id.*, 25:3-6. "[T]he user can select type 742 for limiting what applications (including individual applications) can do on the Internet." *Id.*, 25:10-13. A POSITA would have recognized such access rights are examples of features enabled through the types of policy evaluation described in Rao.

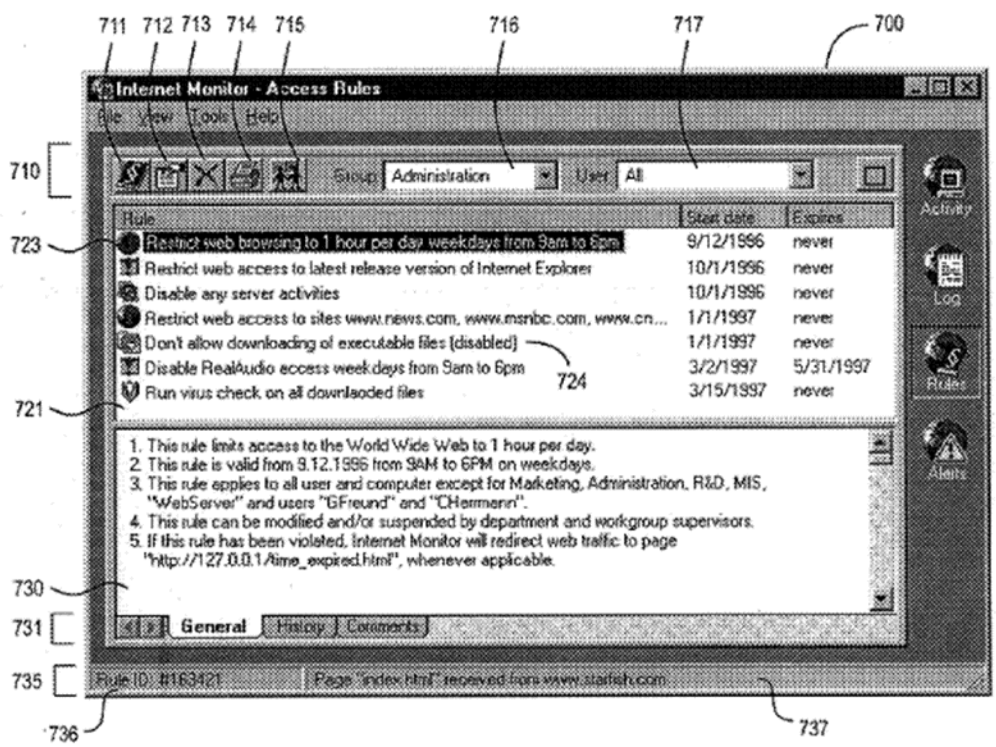
4. ***Claim 4***

[4] The wireless end-user device of claim 1, further comprising a user interface to inform the user of the device when there are options to set, control, override, or modify service usage controls that affect the first differential traffic control policy.

102. As discussed for [3], the Rao-Oestvall device would have incorporated the functionality to output a user interface relating to various aspects of policies used for prioritization, including options for setting how policies are used for prioritization ("***options to set, control override, or modify service usage controls***"). From Rao, "agent 326 may provide a configuration mechanism such as a user interface, graphical or otherwise, design and constructed for configuring or specifying the policies 520." SAMSUNG-1005, [0183]. Based on this disclosure, POSITA would have found it obvious to configure the agent 326 in the Rao-Oestvall device to similarly provide a user interface for "configuring or specifying" policies for prioritization. A POSITA would have also found obvious that the configuration or specification of policies represent "***service usage controls***" since

they can be customized and/or modified to affect the evaluation of policies ("***affect the first differential traffic control policy***"). *Id*.

103. User interfaces for configuring the types of policies described in Rao were well-known before the Critical Date. For example, Freund (SAMSUNG-1010) includes Figure 7A illustrating an example user interface:



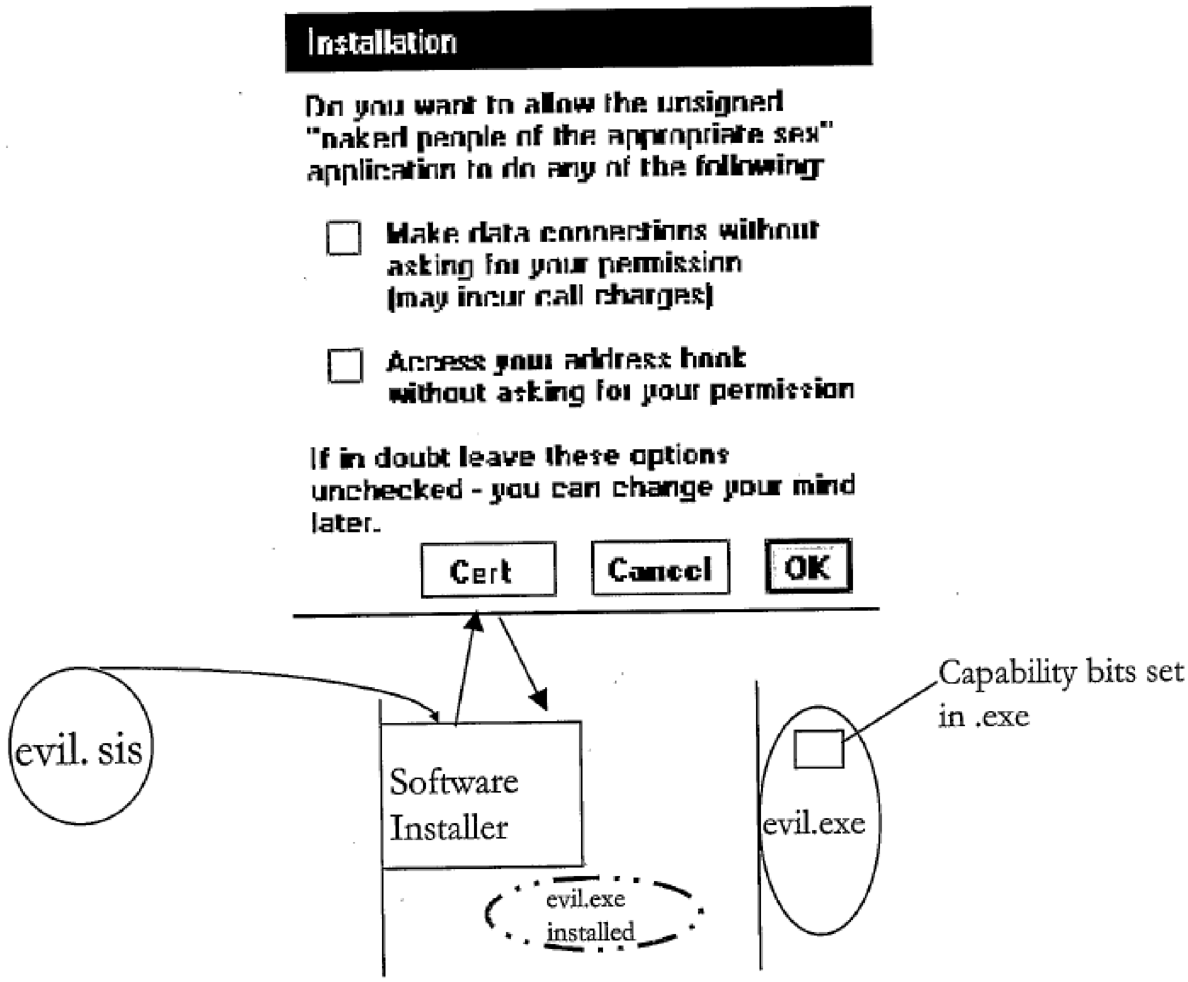
SAMSUNG-1010, FIG. 7A

104. Freund further states, "FIGS. 7A-K illustrate a preferred user interface or 'wizard' dialogs for configuring rules, and "in FIG. 7A, a preferred interface 700 provides a 'view' of rules governing operation of the Internet access monitor, displaying all of the rules which are available for a current configuration."

SAMSUNG-1010, 24:16-20. Freund further teaches that the policies (rules) can be associated with applications using the "wizard dialog 740 [that] asks the user what kind or type of new rule should be created." *Id.*, 25:1-3, FIGS. 7A-K. Freund further teaches that "any given rule is a combination of access rights granted on the basis of available applications, permitted time limits, permitted user activities, permitted protocols, and the like." *Id.*, 25:3-6. "[T]he user can select type 742 for limiting what applications (including individual applications) can do on the Internet." *Id.*, 25:10-13. A POSITA would have recognized such access rights are examples of features enabled through the types of policy evaluation described in Rao.

105. As another example, as discussed for [1.8(a)], Oestvall incorporates by reference Dive-Reclus, which teaches blocking an "unsigned" and provides an interface requesting a user to confirmation whether the application should be blocked. SAMSUNG-1026, 19:17-25, FIG. 2. As shown in Figure 2 (below), a user interface provides a user with information relating to whether an unsigned application should be granted network access without permission by the user.

Figure 2



SAMSUNG-1026, FIG. 2

5. ***Claim 8***

[8.1], [8.2], [8.3] The wireless end-user device of claim 1, wherein the one or more processors are further configured to classify whether a second end-user application is interacting in the device display foreground with the user,

106. Rao-Oestvall would have been configured to apply prioritization to multiple applications, and a POSITA would have found obvious that the

combination renders elements of claim 8 obvious in the same manner as explained above for the "***first end-user application***" based on the disclosures identified in the corresponding claim 1 limitations listed in the table below.

Claim 1 Limitation	Corresponding Limitations
[1.6]	[8.1]
[1.7]	[8.2]
[1.8(a)]	[8.3]

107. As discussed for [1.6], [1.7], and [1.8(a)], a POSITA would have configured the Rao-Oestvall device to perform various types of prioritizations, such as those based on network packet transmission (as described in Rao) and others based on the classification of an application associated with the network packet transmission (as described in Oestvall).

108. Neither Rao nor Oestvall indicate that their respective prioritization techniques are limited to any specific application (or any specific type of application). Oestvall describes "trusted" and "untrusted" applications and teaches applying different access policies for each, rendering this claim obvious. SAMSUNG-1006, [0020]. Rao also teaches that policies "may be specified hierarchically to account for multiple applications 338a-338n and/or multiple protocols that may be executed on the client 105 at any point." SAMSUNG-1005,

[0182]. Rao-Oestvall would have been configured to apply prioritization to multiple applications.

6. ***Claim 9***

[9] The wireless end-user device of claim 1, further comprising a network stack interface integrated with the API.

109. As discussed for [1.8(a)], in Rao-Oestvall, an improved agent would have leveraged several types of APIs (including the recited "***API***") in regulating applications. SAMSUNG-1005, [0110], [0166], [0190], [0205]. In Rao, agent 326 is part of a "network stack" ("***networking stack***") with "network layers," including "applications 338a-338n," "gateway 340," "peer computing device," and "remote access client 120." *Id.*, [0185]. For example, "stacks 310a and 310b" are "network stacks of computing devices 102a-120b or gateway 340, such as any of the computing devices 102 and the gateway 340 illustrated in FIGS. 1A-1C, 2A, or 5A." *Id.*, [0196]. Through these disclosures, a POSITA would have understood and found obvious that the improved agent in Rao-Oestvall (an element of Rao's Figure 5A environment) is part of the network stacks described in Rao. Agent 326 is configured to communicate via an API. A POSITA would have understood and found obvious that a network stack including the agent 326 is "***integrated with***" the API. SAMSUNG-1005, [0106], [0166], [0190], [0203].

110. For example, in Rao, "[an] application hooking is implemented via an application programming interface (API)," so that "the hooking of network packets

occurs at the network layer of the network stack 310a-310n." SAMSUNG-1005, [0166]. Rao also discusses a network architecture of a "network stack." *Id.*, [0100]. In Rao, the "network stack" includes (1) one or more network layers, such as any networks layers of the Open Systems Interconnection (OSI) communications model as those skilled in the art will recognize and appreciate," (2) "one or more protocols, such as the TCP/IP protocol over Ethernet or a wireless protocol, such as IEEE 802.11, as those skilled in the art will recognize and appreciate," and (3) "one or more network drivers supporting the one or more layers, such as a TCP driver or a network layer driver." SAMSUNG-1005, [0100]. The network drives "may be included as part of the operating system of the computing device 102 or as part of any network interface cards or other network access components of the computing device 102," and "may be customized, modified or adapted to provide a custom or modified portion of the network stack 310 in support of any of the techniques of the present invention described herein." *Id.* From these disclosures, a POSITA would have understood and found obvious that Rao-Oestvall-Montemurro's device includes a "***network stack interface integrated with the API***"

111. Network configurations similar to those described in Rao in which an API is "integrated with" a networking stack were also conventional by the Critical Date. For example, "Portable Operating System Interface" (POSIX) is a family of

standards specified by the IEEE to maintain compatibility between operating systems. POSIX defines the application programming interface (API), along with command line shells and utility interfaces, for software compatibility with variants of Unix and other operating systems. SAMSUNG-1021, 104. A POSITA would have understood that a network stack is implemented within the kernel and the stacks interface for making connections and sending and receiving data is made available through systems calls (e.g., connect, send, receive socket calls). System calls are the APIs by which applications access operating system functions. Hence, system calls represent a network stack interface integrated with an API. *Id.*, 69, 104.

7. ***Claim 10***

[10] The wireless end-user device of claim 1, further comprising a networking stack, wherein the one or more processors are further configured to, at an application service interface layer, identify application traffic flows prior to the flows entering the networking stack.

112. As described for [9], Rao-Oestvall would have been configured to operate within one of Rao's network stacks ("***networking stack***"). SAMSUNG-1005, [0185], [0190], [0196], FIG. 3A. The network stacks include at least an "application layer" ("***application service interface layer***") that, for example, allows applications 338a-338n to establish "an application level session." SAMSUNG-1005, [0203]; *see also id.*, [0100], [0133], [0198].

113. A POSITA would have understood and found obvious that packet interception, as provided by Rao-Oestvall, involves identifying the traffic of data generated by applications ("***identify[ing] application traffic flows***") since a processor identifies a packet in the process of determining that the identified packet should be intercepted. Rao provides several packet intercepting techniques, each of which a POSITA would have understood and found obvious involves identifying packets (examples of application traffic flows). *See, e.g.*, SAMSUNG-1005, [0110], [0111], [0137], [0143], [0158].

114. A POSITA would have found also obvious that Rao-Oestvall is configured to "***identify application traffic flows prior to flows entering the network stack***" through Rao's disclosure of a filter process 322 intercepting a network packet "before [the packet] reaches the network stack 310a-310b." SAMSUNG-1005, [0166]. A POSITA would have understood and found obvious that, based on the architectures disclosed in Rao (e.g., Figures 3A, 6A), packet interception (and packet identification) occurs at the "application layer" ("***application service interface layer***"), which sits at a general network layer architecture.

8. ***Claim 13***

[13] The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change the application of the first differential traffic control policy based on a device usage state.

115. As described in Section XI.A, a POSITA would have configured Rao-Oestvall to apply policies based on monitoring a state and classification of an application. A POSITA would have understood and found obvious that the present interaction state represents an example of "***device usage state***" as it indicates whether the application is currently made available for display on a mobile device, and therefore, available for active use by a user. A POSITA would have known that device usage state can include which applications are executing, including whether each application is executing in the foreground or background. A POSITA would have known that systems routinely monitored which application were running.

116. For example, in Rao, an application is not in the background if it is "currently in active use by the user." SAMSUNG-1005, [0003]. A POSITA would have recognized that the Rao device performs ongoing monitoring of which applications are running, and which are running in the foreground and background, so it can dynamically determine whether to apply the Internet access controls. SAMSUNG-1005, [0182], [0188]. Rao teaches that "the policies 520 define prioritization based on whether an application is running in the foreground or the

background of the client 105." SAMSUNG-1005, [0182]. Rao additionally teaches "the remote access client 120 may have one or more policies 520 for specifying client-side prioritization of network communications related to applications 338a-338n running on application" and "may determine whether the application 338a-338n associated with the network packet is running in the foreground or the background of the client 105." SAMSUNG-1005, [0182], [0188]. A POSITA would have recognized that the Rao device performs ongoing monitoring of which applications are running, and which are running in the foreground and background, so it can dynamically determine whether to apply policies. *Id*. For example, "the remote access client 120 may determine whether the application 338a–338n associated with the network packet is running in the foreground or the background of the client 105." *Id.* Here, detecting (and reacting to the detection) is necessarily a dynamic operation. Note that the enforcement of policies using ongoing monitoring was a common practice in 2009 (and before). For example, it was common for operating systems to recover disk space by removing unused or important files when it determined disk space was running low.

117. Rao also includes as examples of device usage states relating to the network such as congestion state. *Id.*, [0195]. For example, Rao explains that the device performs ongoing monitoring of the device state, e.g., "the remote access client 120 may receive an indication of network congestion, such as receiving a

window size of zero for a TCP connection related to an application 338a-338n," "the remote access client 120 may recognize a high number of retransmits to a particular destination," and "the client 105 controls and manages the prioritization of network communications of the client 105 on an application 338 a-338 n basis and in accordance with any policies 520 for the client 105 and in further view of any network statistics and other factors occurring on the network.SAMSUNG-1005, [0195].

118. Likewise, in Oestvall, an untrusted application is deemed to be in the background if "the display shows a screen saver or is actually turned off." SAMSUNG-1006, [0024]. Oestvall also describes preventing an untrusted application from "being given any services or consuming any resources" based on whether the application is "in the background or foreground on display." SAMSUNG-1006, [0023].

119. Based on these disclosures, Rao-Oestvall device would have been configured to adjust policy evaluation relating to application-related prioritization ("***dynamically change the application of the first differential traffic control policy based on a device usage state***") based on the application's present interaction state ("***device usage state***").

9. ***Claim 14***

[14] The wireless end-user device of claim 1, wherein the one or more processors configured to classify whether or not the first end-user application, when running, in interacting in the device display foreground with a user perform the classification based at least in part on a state of user interface priority for the application.

120. As described in Section XI.A, a POSITA would have configured Rao-Oestvall to apply policies based on monitoring a state and classification of an application. A POSITA would have understood and found obvious that a present interaction state of an application (foreground, background) represents an example of a "***state of user interface priority for the application***." An application's present interaction state indicates whether the application is prioritized for display on a mobile device. Oestvall recognizes that "[i]n conventional multi-tasking computers running several different applications at the same time, an application will issue a software interrupt to the operating system," and "interrupts from different applications are prioritised and queued by an interrupt handler." SAMSUNG-1006, [0005]. Oestvall also teaches prioritization based on a "trust" classification of an application, which a POSITA would have understood and found obvious is another example of a "***state of user interface priority***." *Id.*, [0015].

121. Similarly, Rao describes that policies "define prioritization based on whether an application is running in the foreground or the background of the client 105." SAMSUNG-1005, [0182]. A POSITA would have found obvious that Rao-

Oestvall applies policies to perform application-related prioritization based on the various examples of present interaction states described in Rao and Oesvall (“***classify whether or not the first end-user application***” is “***interacting in the device display foreground with a user***”). For example, Rao indicates that an application in the foreground is one that is “currently in active use by the user,” which a POSITA would have understood and found obvious indicates a user interface priority in that the application is prioritized over other applications that are running in the background. SAMSUNG-1005,[0182].

122. The use of user interface priority in coordinating application operation was well-known before the Critical Date. For example, Singh (SAMSUNG-1013) describes a “window management function [that] determine[s] a relationship of windows with one another.” SAMSUNG-1013, 9:19-21. Singh teaches that “when a user interacts with a window, the window becomes the highest priority window.” *Id.*, 9:33-35. A POSITA would have known that users interact with foreground windows, and in Singh, users only interact with the highest priority window (because any interaction causes the window to be assigned the highest priority). A POSITA would have understood or found obvious that Singh’s window management function uses a state of user interface priority (e.g., the highest priority, which is defined to be the one the user is interacting with, also known as

having interface focus) to classify that the application is interacting with the user in the UI foreground. *Id.*

123. In addition, the difference between foreground and background states has been well established within the academic literature. For example, in 1995, a publication by Buxton described foreground as "activities which are in the fore of human consciousness", such as "speaking on the telephone, or typing into a computer," SAMSUNG-1024, 1. In contrast, background activities are "tasks that take place in the periphery, 'behind those in the foreground'." *Id.* Activities in the "fore of human consciousness" would indicate user interface priority. *Id.* As another example, a publication by Hinckley built on this model in 2005 to further define foreground concerns as "deliberate user activity where the user is attending to the device" and background as "the realm of inattention or split attention," which makes the user interface priority with regards to foreground actions even more explicit. SAMSUNG-1025, 1.

124. The Rao-Oestvall device would have been configured to apply a policy to perform application-related prioritization based on the application's present interaction state ("***configured to classify whether or not the first end-user application, when running, in interacting in the device display foreground with a user perform the classification based at least in part on a state of user interface priority for the application***").

10. ***Claim 16***

[16] The wireless end-user device of claim 1, wherein the one or more processors are configured to associate the first end-user application with the first differential traffic control policy based on an application behavior.

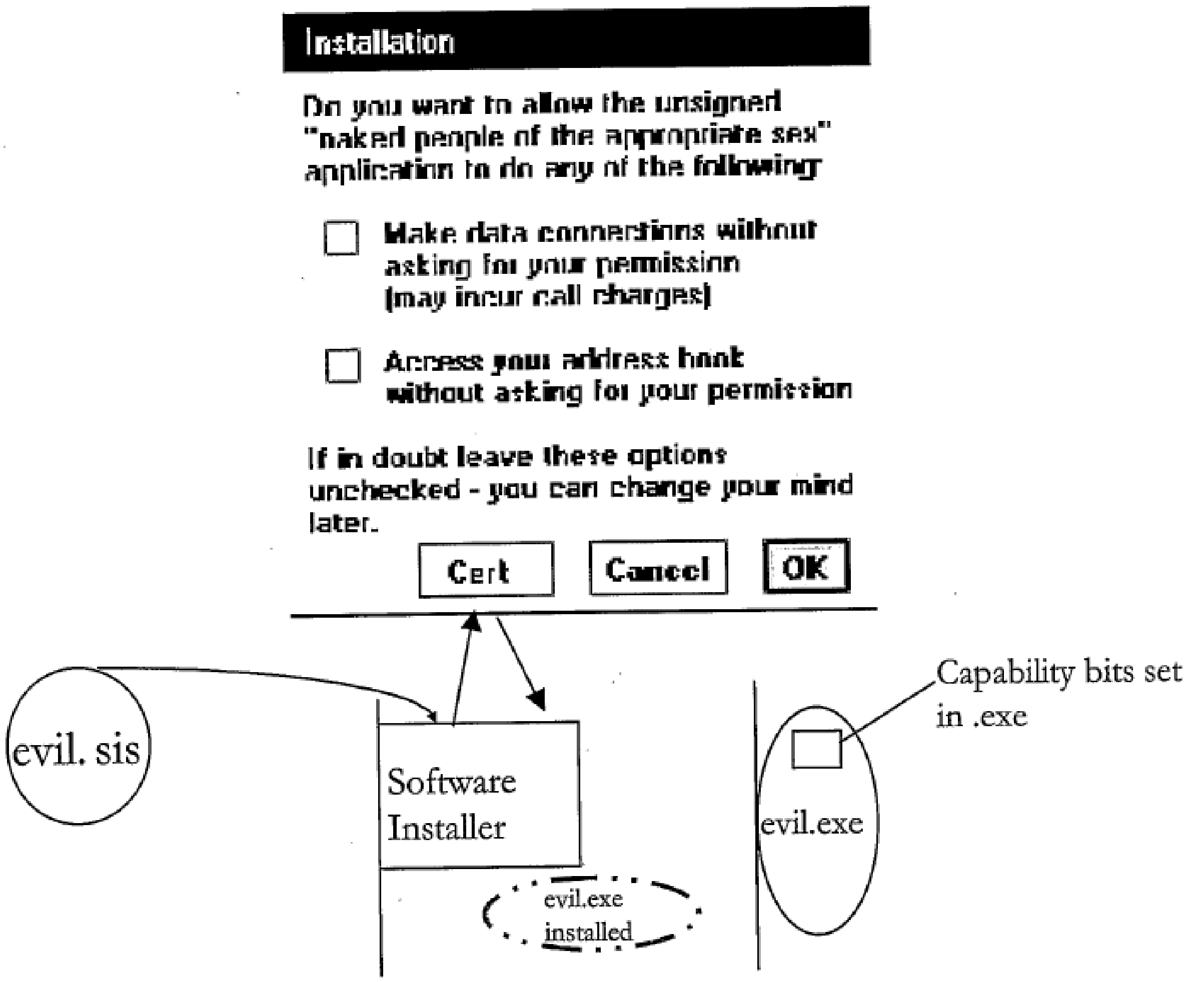
125. As described in Section XI.A, a POSITA would have configured Rao-Oestvall to apply policies based on monitoring a state and classification of an application. Oestvall describes preventing an untrusted application from "being given any services or consuming any resources" based on whether the application is "in the background or foreground on display." SAMSUNG-1006, [0023]. A POSITA would have understood and found obvious that a present interaction state of an application (foreground, background) represents an example of "***application behavior.***" An application's present interaction state indicates whether the application is currently made available for display on a mobile device. For example, in Oestvall, an untrusted application is deemed to be in the background if "the display shows a screen saver or is actually turned off." SAMSUNG-1006, [0024]. Likewise, in Rao, an application is in the background if it is "currently in active use by the user." SAMSUNG-1005, [0003]. The Rao-Oestvall device would have been configured to apply a policy to perform application-related prioritization based on the application's present interaction state ("***configured to associate the first end-user application with the first differential traffic control policy based on an application behavior***").

11. ***Claim 19***

[19] The wireless end-user device of claim 1, further comprising an agent to block, modify, remove, or replace, based on the applied differential traffic control policy, user interface messages generated by the first end-user application.

126. Rao-Oestvall would have included an improved agent ("***agent***") for performing various management operations for applying policies for packet-related and application-related prioritization. SAMSUNG-1005, [0182]; SAMSUNG-1006, [0023]. As discussed in Section XI.A and [1.8(a)], a POSITA would have configured the improved agent to prevent an untrusted application from running or being given access to a service that consumes resources. *Id.* In Oestvall, this is accomplished by sending a "control signal" to prevent application functionality. SAMSUNG-1006, [0023]. A POSITA would have understood and found obvious that such restriction would have precluded an application from sending user interface messages (e.g., "***block, modify, remove, or replace…user interface messages generated by the first end-user application***"). For example, as Oestvall describes, the restriction denies "system resources" and "CPU activity" that would have been necessary for an application to generate and output user interface messages. SAMSUNG-1006, [0021]. As another example, Oestvall incorporates by reference Dive-Reclus, which teaches blocking an "unsigned" application and provides an interface requesting a user to confirmation whether the application should be blocked. SAMSUNG-1026, 19:17-25, FIG. 2.

Figure 2



SAMSUNG-1026, FIG. 2

12. ***Claim 20***

[20] The wireless end-user device of claim 1, wherein the one or more processors configured to apply the first differential traffic control policy to disallow Internet service activity on behalf of the first end-user application perform a disallowance of Internet service activity by intercepting open,

connect, and/or write requests by the first end-user application to a network stack.

127. As discussed for [1.7], Rao-Oestvall renders obvious that application-related prioritization results in "***Internet service activity on behalf of the [application 338]***" being "***disallowed***." Rao-Oestvall incorporates Rao's packet-related prioritization techniques, which includes "intercepting network traffic of any of the applications 338a–338n," and, involves "***intercepting open, connect, and/or write requests by the first end-user application to a network stack***." SAMSUNG-1005, [0024]-[0031], [0106], [0166], [0180], [0184], [0185], [0190], [0196], [0203].

13. ***Claim 25***

[25] The wireless end-user device of claim 1, wherein the API comprises a network access API.

128. As discussed for [1.8(a)], in Rao-Oestvall, an improved agent would have leveraged several types of APIs (including the recited "***API***") in regulating applications. SAMSUNG-1005, [0110], [0166], [0190], [0205]. For example, Rao describes use of a "hooking application programming interface (API) to intercept, hook, or otherwise obtain inbound and/or outbound packets of the client 105, such as the network traffic associated with application 338." SAMSUNG-1005, [0110]. Based on this disclosure, a POSITA would have understood and found obvious that the APIs leveraged by the improved agent in Rao-Oestvall includes a "***network***

access API." As another example, Oestvall incorporates by reference Dive-Reclus, which teaches using permissions to regulate API calls (e.g., granting, blocking) made by applications in accessing a network. SAMSUNG-1006, [0020]; SAMSUNG-1026, 16:23-17:28. This coincides with the '976 patent specification's disclosure that "network access API" is "used to implement traffic control for network capacity controlled services." SAMSUNG-1001, 92:1-26.

14. ***Claim 27***

[27] The wireless end-user device of claim 1, wherein the API informs the first end-user application when it is allowed to access Internet data service that is available via the WWAN modem.

129. As discussed for [1.8(a)] and [1.8(c)], in Rao-Oestvall, an improved agent would have leveraged several types of APIs (including the recited "***API***") in regulating applications. SAMSUNG-1005, [0110], [0166], [0190], [0205]. A POSITA would have understood and found obvious that APIs leveraged by the improved agent of Rao-Oestvall includes conventional APIs known by the Critical Date, such as a Java sockets API through which an application communicates data over a network. SAMSUNG-1020, 3-4. For example, when a network access condition is used to permit an application to access the network, a POSITA would have understood and found obvious that the Java sockets API provides an indication to the application of the network access condition ("***the API informs the first end-user application when it is allowed to access Internet data service that is***

available via the WWAN modem”). Such a configuration would have supported Oestvall’s disclosure that “[w]hen the untrusted application is brought to the foreground again, it is allowed to run again.” SAMSUNG-1006, [0021]. As another example, Oestvall incorporates by reference Dive-Reclus (SAMSUNG-1026), which teaches using permissions to regulate API calls (e.g., granting, blocking) made by applications in accessing a network and a POSITA would have found it obvious that granting or blocking permission for an API call by an application involves providing an indication to the application regarding the permission through the called API. SAMSUNG-1026, 16:23-17:28, 20).

15. ***Claim 28***

[28] The wireless end-user device of claim 1, wherein the API informs the first end-user application of one or more network traffic controls that the first end-user application is expected to implement.

130. As discussed for [1.8(a)], in Rao-Oestvall, an improved agent would have leveraged several types of APIs (including the recited “***API***”) in regulating applications. SAMSUNG-1005, [0110], [0166], [0190], [0205]. A POSITA would have understood and found obvious that APIs leveraged by the improved agent of Rao-Oestvall includes conventional APIs known by the Critical Date, such as a Java sockets API through which an application communicates data over a network. SAMSUNG-1020, 3-4. In Oestvall, when an application running in the background requests network access, the application is denied access to system resources

(including network access resources), which results in the application being informed of one or more network traffic controls that the application is expected to implement. SAMSUNG-1006, [0023]. Oestvall also incorporates by reference Dive-Reclus, which teaches permission decisions regulating network access by third-party applications that use API calls. *Id.*, [0020]; SAMSUNG-1026, 16:23-17:28, 20. A POSITA would have found it obvious that a permission decision is an example of "***one or more network traffic controls***" that controls network access, which is communicated to the application through a corresponding API ("***API informs the first end-user application of one or more network traffic controls***"). SAMSUNG-1006, [0020]; SAMSUNG-1026, 16:23-17:28, 20.

131. For example, a POSITA would have understood that one or more instructions provided by the API to enable or restrict the application's access to network resources (and thereby the application's access to outputting or receiving any network traffic). Specifically, a POSITA would have also recognized that instructions provided by the API is capable of opening connections, sending and receiving data, and closing connections, each of which involves controlling when these network operations by an application occur and how they are handled. In this sense, instructions provided by the Java Sockets API controls an application's access to network resources and thereby represents "***one or more network traffic controls***." Such a configuration would have supported Oestvall's disclosure that

"[w]hen the untrusted application is brought to the foreground again, it is allowed to run again." SAMSUNG-1006, [0021], [0023]; SAMSUNG-1018, 15:44-55.

XI. [GROUND 1B] ‑ RAO-OESTVALL-MONTEMURRO MAKES CLAIMS 5-7, 11, 17, 18, 23, 24, AND 26 OBVIOUS

A. Combination of Rao, Oestvall, and Montemurro

132. As described in Section XI.A, a POSITA would have configured Rao-Oestvall to apply policies to prioritize packet transmission and application functionality to achieve several types of operational efficiencies. SAMSUNG-1005, [0179]-[0195], FIG. 5A. In implementing this combination, a POSITA would have recognized opportunities to provide additional efficiencies in scenarios where the Rao-Oestvall device has access to multiple networks. *Id.* This would have motivated a POSITA to seek solutions beyond Rao and Oestvall to achieve such additional efficiencies. *Id.*

133. Given Montemurro's broad focus to "optimize communications using a policy-based mechanism to configure connections and routes," a POSITA would have found Montemurro's teachings to be applicable to the policies applied by Rao-Oestvall for prioritization. Indeed, Like Oestvall, Montemurro describes embodiments where its policies are used to "disable or enable an application for a user." SAMSUNG-1007, [0027]. This would have led a POSITA to consider Montemurro's broader teachings in Figure 2 relating to "policy-based data routing for multimode operations." *Id.*, [0024]; SAMSUNG-1007, [0024]. Incorporation of

such teachings into Rao-Oestvall would have yielded several of improvements described in Montemurro, such as the ability to "offer different usage models depending on the mode of wireless operation selected." *Id.*, [0003]. This configuration would have improved the Rao-Oestvall device by enabling prioritization to further account for several considerations, such as "bandwidth, range, cost, and power consumption." *Id.*

134. A POSITA would have had a reasonable expectation of success in combining Rao-Oestvall and Montemurro, as discussed above. For example, Rao provides non-limiting disclosure of the types of networks to which device 102 may connect to using network interface 118. SAMSUNG-1005, [0095], [0125]. Montemurro's use of routing tables would have thereby advanced Rao's motivation to enable multiple types of network connectivity. SAMSUNG-1007, [0024]. Additionally, both Rao and Montemurro expressly teach use of policies to regulate device functions (e.g., prioritizing network traffic in Rao, connecting to a suitable available network in Montemurro). SAMSUNG-1005, [0182]; SAMSUNG-1007, [0011]. A POSITA would have understood these disclosures to both be generally focused on improving network performance on a mobile device, making the combination of their teachings a natural option to achieve the advantages discussed above. Additionally, configuring Rao-Oestvall to leverage Montemurro's teachings would have required only routine programming

knowledge well within the skill of a POSITA prior to the earliest effective filing date. The change would have involved (1) combining prior art elements according to known methods to yield predictable results; and (2) use of a known technique to improve similar devices (methods, or products) in the same way. For example, Rao-Oestvall-Montemurro would have provided a device that uses a set of policies to generally regulate applications, including policies used to prioritize network packet transmissions (as described in Rao) and policies used to select the most suitable network connection (as described in Montemurro).

B. Analysis of Claims 5-7, 11, 17, 18, 23, 24, and 26

1. *Claim 5*

[5] The wireless end-user device of claim 1, wherein the first differential traffic control policy is part of a multimode profile having different policies for different networks.

135. Rao-Oestvall-Montemurro would have incorporated the functionality described in Montemurro to apply a rules engine to coordinate connectivity for applications. SAMSUNG-1007, [0027]. As described in Section XII.A, in certain scenarios, a rules engine would have applied an instance of a routing table ("***multimode profile***") with information for multiple networks available for selection. *Id.*, [0030]. For example, "if both the WLAN and WWAN radios…of [a] device [] are connected to their respective networks 104 and 106, there will be a route associated with each network 104 and 106…" *Id.* The rules engine

"executes" an instance of the routing table "to ensure that data goes out to the most appropriate network" and also to "determine which interface would be best used to service a particular application." *Id.*, [0035].

136. In scenarios where multiple networks are available for selections, a POSITA would have understood and found obvious that the information specified by the instance of the routing table includes policies for each available network. In Montemurro, policies are "responsive to various factors such as Radio Access Technology, high/low bandwidth, cost, presence, time of day, location, application type and quality of service (QoS) requirements." SAMSUNG-1007, [0011], [0024], [0027], [0029]. Thus, a POSITA would have understood and found obvious that the instance of the routing table with information for multiple networks available for selection thereby includes "***different policies for different networks***." SAMSUNG-1007, [0011], [0024], [0027], [0029].

137. The use of different policies for enabling capabilities for different networks (e.g., phone network, local network) was conventional by the Critical Date. SAMSUNG-1026, 12:13-13:9. For example, Dive-Reclus (SAMSUNG-1026) includes a table showing different permission decisions for applications

submitting API calls to request network access.

Installed	PhoneNetwork	ReadUserData	WriteUserData	LocalNetwork	Certificate
Good.exe	Not granted	Granted	Not granted	Granted	Checked OK – click to view root signing cert
Bad.exe	Not granted	Not granted	Not granted	Not granted	Unsigned

SAMSUNG-1026, 20

2. *Claim 6*

[6] The wireless end-user device of claim 5, wherein the one or more processors are further configured to select a traffic control policy from the multimode profile based at least in part on the type of network connection currently in use by the device.

138. As described for [5], in Rao-Oestvall-Montemurro, a rules engine, in certain scenarios, applies an instance of a routing table ("***multimode profile***") with information for multiple networks available for selection. SAMSUNG-1007, [0011], [0024], [0027], [0029]. A POSITA would have also understood and found obvious that, in these scenarios, the information specified by the instance of the routing table includes "***different policies for different networks***." *Id.* The rules engine "executes" an instance of the routing table "to ensure that data goes out to the most appropriate network" and also to "determine which interface would be best used to service a particular application." *Id.*, [0035]. For example, "if both the

WLAN and WWAN radios…of [a] device [] are connected to their respective networks 104 and 106, there will be a route associated with each network 104 and 106…" *Id.*, [0030]. In this example, a POSITA would have understood and found obvious that the rules engine within Rao-Oestvall-Montemurro would have executed the instance of the routing table based on types of current network connections of a device (WLAN, WWAN). When a routing option is selected from the routing table instance, the selection ("***select a traffic control policy***") is based on the types of current network connections of the device ("***type of network connection currently in use by the device***"). In addition, Montemurro describes performance criteria based on the type of network connection currently used by the device, and if these criteria are not maintained, "alternatives for the present access technology or different instance of the same type of access technology (e.g., a different WLAN or subnetwork via an alternative access point, PPP connection or GSM APN) can be evaluated." *Id.*, [0044].

139. Additionally, as discussed for [1.8(a)] (Ground 1A), Oestvall incorporates by reference Dive-Reclus, which teaches permission decisions regulating network access by third-party applications that use API calls. SAMSUNG-1006, [0020]; SAMSUNG-1026, 16:23-17:28, 20.

3. *Claim 7*

[7] The wireless end-user device of claim 6, wherein the one or more processors are further configured to, when the type of network connection is at least one type of WLAN connection, select a traffic control policy from the multimode profile based at least in part on a type of network connection from the WLAN to the Internet.

140. *See* [6] above. Montemurro offers an example in which "if both the WLAN and WWAN radios…of [a] device [] are connected to their respective networks 104 and 106, there will be a route associated with each network 104 and 106…" *Id.* In this example, a POSITA would have understood and found obvious that the rules engine within Rao-Oestvall-Montemurro would have executed the instance of the routing table ("***select a traffic control policy from the multimode profile***") when the device is connected to a WLAN connection ("***when the type of network connection is at least one type of WLAN connection***"). Additionally, as described above, Montemurro describes performance criteria based on the type of network connection currently used by the device and specifically considers when the device is connected to a WLAN connection. If the performance criteria are not maintained, "alternatives for the present access technology or different instance of the same type of access technology (e.g.***, a different WLAN or subnetwork via an alternative access point***, PPP connection or GSM APN) can be evaluated." *Id.*, [0044]. (Emphasis added.)

141. Montemurro also describes that "once work hours end, a rule could be triggered, for example, by a calendar application, to change the default route so that traffic is routed across the local LAN rather than the corporate network" and that "[i]f the user is at work, there could be another rule to disable this default route change." SAMSUNG-1007, [0039]. From this disclosure, a POSITA would have understood and found obvious that the "local LAN" is a type of network connection from the WLAN to the Internet. For example, Montemurro describes that its device "is capable of wireless communication in accordance with WLAN" and "communicate[s] through cellular network 104 and a representative base station 108 coupled to the Internet 112 and/or through WLAN or WMAN network 106 and its access point 110 also coupled to Internet 112." SAMSUNG-1007, [0013]. A POSITA would have understood and found obvious that there would be several types of network connections implemented by various network components (e.g., base station, various WLAN components, access points, etc.) between the WLAN and the Internet, and that Rao-Oestvall-Montemurro's device would consider a ***type*** of such network connection in ***selecting a traffic control policy from the multimode profile***, as discussed above.

4. ***Claim 11***

[11] The wireless end-user device of claim 1, wherein the one or more processors apply the first differential traffic control policy to one of but not

both of a connection to a roaming WWAN network and a connection to a home WWAN network.

142. As described for [5], in Rao-Oestvall-Montemurro, a rules engine, in certain scenarios, applies an instance of a routing table ("***multimode profile***") with information for multiple networks available for selection. SAMSUNG-1007, [0011], [0024], [0027], [0029]. Policies are "responsive to various factors," including "cost, presence, time of data, location, e.g., geo-based policies, network roaming)." *Id.*, [0029]. Montemurro also offers non-limiting disclosure of WWAN, including examples of "cellular technologies like GSM/GPRS EDGE, UTMS, HSPA, CDMA, WCDMA, etc.," which a POSITA would have understood and found obvious includes roaming WWAN networks and home WWAN networks. A POSITA would have perceived selection of a policy in Rao-Oestvall-Montemurro to provide connectivity to one of several available WWAN networks ("***apply the first differential policy to one of but not both of a connection to a roaming WWAN network and a connection to a home WWAN network***") to represent an obvious configuration as this reduces costs and complexity, consistent with Montemurro's teachings. SAMSUNG-1007, [0029]-[0038].

143. For example, it was well-known and obvious to use and make selective connection to a home network (e.g., "home WWAN") and a roaming network (e.g., roaming WWAN) for similar advantages such as cost. SAMSUNG-

1022, [0003] ("A wireless device is typically associated with a home network operator and, when available, uses the home network for wireless communications. The home network operator may have partner network operators that provide roaming service to the wireless device. That is, the roaming network operators permit the wireless device to connect to the home network via the roaming network when the wireless device is outside of the device's home network's coverage area. A user may desire certain information (such as cost) as an aid to deciding whether to connect to a roaming network, and/or as an aid to deciding to which roaming network to connect."), [0004] ("Typically, to establish a data connection with a home WWAN, a wireless device needs to have certain information.").

144. Systems and techniques for enabling policy-based connectivity to roaming and home networks were also conventional by the Critical Date. For example, U.S. Pat. App. No. 2008/0311897 to Segal describes a system that can activate international roaming services using an availability policy. SAMSUNG-1023, Abstract, FIG. 3, [0043]. The system also communicates with a subscriber to update network communication services, which allows a subscriber to roam internationally. *Id.* As shown in FIG. 3, a user may select a policy when presented with it such an option:

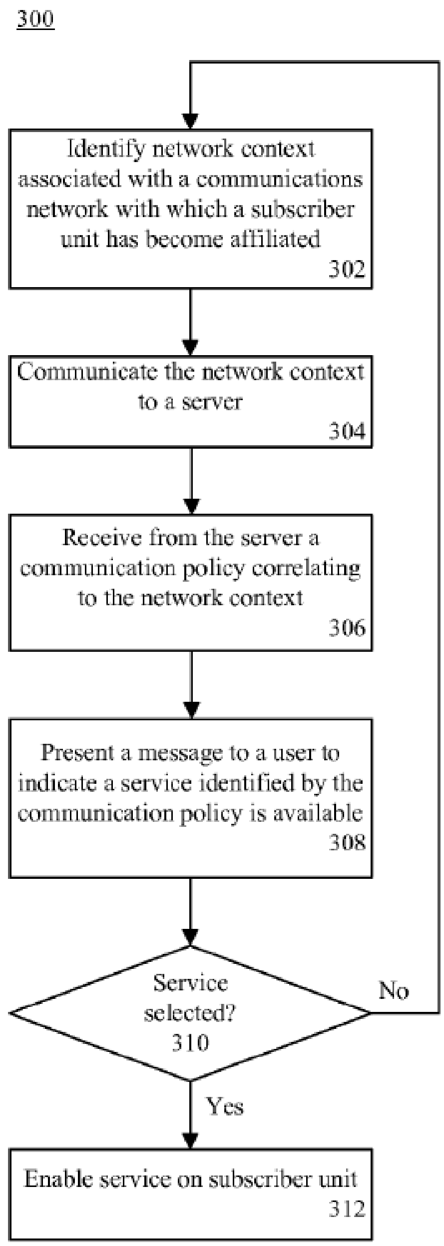


FIG. 3

SAMSUNG-1023, FIG. 3

5. ***Claim 17***

[17] The wireless end-user device of claim 1, wherein the differential traffic control policy defines that applications to which the policy applies can only have WWAN network access events during particular time windows.

145. As discussed for [5], in Rao-Oestvall-Montemurro, a rules engine, in certain scenarios, applies an instance of a routing table ("***multimode profile***") with information for multiple networks available for selection. SAMSUNG-1007, [0011], [0024], [0027], [0029]. Policies are "responsive to various factors," including "cost, presence, time of data, location, e.g., geo-based policies, network roaming)." *Id.*, [0029]. The rules engine "executes" the instance of the routing table to "ensure that data goes out to the most appropriate network (via respective network interface)" and "interacts with the connection API's to determine which interface would be best used to service a particular application." *Id.*, [0035]. A POSITA would have understood and found obvious that Rao-Oestvall-Montemurro regulates access to connection events to several networks, including a WWAN network ("***WWAN network access events***").

146. As discussed above for [1.8(a)]-[1.8(c)] and Section XII.A, Rao-Oestvall-Montemurro would have regulated network access by applications through use of policies. In Montemurro, "[p]olicies may be responsive to various factors," including "time of day." SAMSUNG-1007, Abstract. A POSITA would have understood and found obvious that a policy applied by Rao-Oestvall-

Montemurro regulates both the type of network access and the circumstances during which an application can have access to network services such that Rao-Oestvall-Montemurro "***can only have WWAN network access during particular time windows***" (e.g., time windows during which a policy specifies network connectivity). SAMSUNG-1006, [0023]; SAMSUNG-1007, [0035].

147. Use of policies to limit network access during particular time windows were Conventional by the Critical Date. For example, Freund describes "access rules can be qualified by optionally specifying: ... **<u>time of day</u>** when the rule should be applied (for example from 9 am to 5 pm)." SAMSUNG-1010, 10:13-17. A POSITA would have understood and found obvious the "access rules" are examples of policies since they can, e.g., "[d]elay Internet access for non-critical Applications or Protocols" and "[d]isable Internet Access for non-critical or Protocols." *Id.*, 30:59-67. In Freund, access rules define when access to the Internet is allowed, and therefore represents, an example of a policy that limits Internet access during a particular time window (e.g., between 9 am and 5 pm).

6. ***Claim 18***

[18] The wireless end-user device of claim 1, wherein the one or more processors are further configured to update the first differential traffic control policy based on information received from a network element.

148. As discussed in Section XI.A, policies applied by Rao-Oestvall-Montemurro (including the "first differential traffic control policy") would have

been "responsive to various factors such as Radio Access Technology (high/low bandwidth), cost, presence, time of day, location, application type and quality of service (QoS) requirements among others to optimize communications," as described in Montemurro. SAMSUNG-1007, [0011].

149. In Montemurro, "network infrastructure" provides support for services provided to a wireless device. *Id.*, [0014]. Examples of "network infrastructure" include "a gateway server, a provisioning server, a discovery, and an application repository," each of which are examples of a "***network element***." Services provided by the network infrastructure include "Administrative and Management Service dealing with policies, such as those specifying allowed applications for users, services available to applications and more." *Id.*, [0015]-[0016].In Rao, remote access client 120 may "receive an indication of network congestion" and thereby "control[] and manage[] the prioritization of network communications," which would have adjusted policy evaluation by the device. SAMSUNG-1005, [0195]. Based on these disclosures, a POSITA would have understood and found obvious, where a server ("***network element***") provides an update for a service dealing with policies, Rao-Oestvall-Montemurro would have been configured to update policies relating to application operation ("***update the first differential traffic control policy***") based on the update from the server ("***information received from [the] network element***"). For example, the update may specify a new allowed

application, and the Rao-Oestvall-Montemurro device would have updated policies to reference a name of the new allowed application and thereby permit regulation of the newly allowed application, consistent with Rao. *See* SAMSUNG-1005, [0182] ("the policies 520 may be specified by the name of the applications 338a-338n and/or the type of application 338a-338n").

150. Techniques for adapting policy configurations based on information received from network elements were conventional by the Critical Date. For example, Freund (SAMSUNG-1010) describes a network element in the form of a "supervisor" that "maintains access rules for the client-based filtering and verifies the existence and proper operation of the client-based filter application." SAMSUNG-1010, Abstract. "The supervisor monitors whether a client has the filter application loaded and **provides the filter application with the rules for the specific user or workstation**." *Id.*, 5:9-12. In Freund, "[c]lient Monitor sends a login request to the Supervisor," and in response, "the Supervisor checks if the Client Monitor (computer/user) has any Internet access rights; also, the Supervisor determines the department or workgroup for the Client Monitor, as indicated at step 805." *Id.*, 28:6-14. Based on these determinations, "the Supervisor filters rules appropriate for the client (i.e., application, Host, and other rules), and transmits them to the Client Monitor, at step 806." *Id.*, 28:14-16. A POSITA would have recognized that the Supervisor is a network element (a service

controller) and "the network service activity control policy set" is updated based on information received from the Supervisor.

151. Freund also describes the "centralized supervisor application is installed on a computer on the LAN that can be reached from all workstations that need access to the Internet; this is typically (although not necessarily) a server computer." SAMSUNG-1010, 5:6-9. In this example, Freund's server represents an example of a network element. This is consistent with the '976 patent specification, which describes an example of a "network element" as "a service controller or another network element/function)." SAMSUNG-1001, 11:31-46.

7. *Claim 23*

[23] The wireless end-user device of claim 1, the first differential traffic control policy comprising first and second sub-policies applicable respectively to Internet data service provided using the WWAN modem to connect to a home WWAN and a roaming WWAN, wherein the one or more processors are further configured to apply the first sub-policy when Internet data service is provided through a home WWAN and to apply the second sub-policy when Internet data service is provided through a roaming WWAN.

152. As discussed for [5], in Rao-Oestvall-Montemurro, a rules engine, in certain scenarios, applies an instance of a routing table ("***multimode profile***") with information for multiple networks available for selection. SAMSUNG-1007, [0011], [0024], [0027], [0029]. For example, "if both the WLAN and WWAN radios…are connected to their respective networks 104 and 106, there will be a

route associated with each network 104 and 106," as shown in the figure below. SAMSUNG-1007, [0030].

Source IP	Destination IP	Device Interface (208)
192.168.1.20	0.0.0.0	WLAN (208A)
67.69.20.142	0.0.0.0	WWAN (208C)

153. In Montemurro, a device "has mobile IP capabilities" to "permit the device to attach to the Internet (IP network) via a home and one or more foreign networks." SAMSUNG-1007, [0037]. Montemurro contemplates devices with capabilities to connect to both home and foreign networks. A POSITA would have found obvious that the routing table may be similarly configured to provide routing options for various types of networks, including a "***home WWAN***" and "***roaming WWAN***." SAMSUNG-1007, [0037].

154. Montemurro's device is operable on various networks (including WWAN). A POSITA would have understood and found it obvious that the routing table is similarly configured to provide routing options for WWAN for a home network ("***home WWAN***") and WWAN for roaming to a foreign network ("***roaming WWAN***"). SAMSUNG-1007, [0030], [0037]. Indeed, by the Critical Date, WWAN was well-known for being implemented for different settings, such

as a home WWAN and a roaming WWAN. Montemurro further also offers non-limiting disclosure of WWAN, e.g., "cellular technologies like GSM/GPRS EDGE, UTMS, HSPA, CDMA, WCDMA, etc.," which a POSITA would have understood and found obvious includes roaming WWAN networks and home WWAN networks. A POSITA would have perceived network selection in Rao-Oestvall-Montemurro to provide connectivity to one of several available WWAN networks ("***connect to a home WWAN and a roaming WWAN***") to represent an obvious configuration as this reduces costs and complexity, consistent with Montemurro. SAMSUNG-1007, [0029]-[0038].

155. It was well-known and obvious to use and make selective connection to a home network (e.g., "***home WWAN***") and a roaming network (e.g., "***roaming WWAN***"). For example, U.S. Pat. App. No. 2009/0093247 ("Srinivasan") describes a system in which "[a] wireless device is typically associated with a home network operator and, when available, uses the home network for wireless communications[,]" where "[the] operator may have partner network operators that provide roaming service to the wireless device." SAMSUNG-1022, [0003]. In this configuration, "the roaming network operators permit[s] the wireless device to connect to the home network via the roaming network when the wireless device is outside of the device's home network's coverage area." *Id.* Further, "[a] user may desire certain information (such as cost) as an aid to deciding whether to connect to

a roaming network, and/or as an aid to deciding to which roaming network to connect" and "[i]n many cases, the wireless device may be programmed with the identity of one or more voice roaming partner operators of its home operator so that a partner voice roaming network operator can be located when the wireless device is outside of the home network's coverage. *Id.*

156. In Montemurro, each policy specifies a set of connection of factors, such as "Radio Access Technology, high/low bandwidth, cost, presence, time of day, location, application type and quality of service (QoS) requirements." SAMSUNG-1007, [0011]. A POSITA would have understood and found obvious that a set of connection factors specified within a policy represents a "***sub-policy***" in that they permit connectivity to an associated network, and thereby enables Montemurro's "policy-based mechanism to configure connections and routes." *Id.*, Abstract. An instance of the routing table with routing options for a home network and a foreign network, the routing table includes a first set of connection factors for the home network ("***first sub-policy when Internet data service is provided through a home WWAN***") and a second set of connection factors for the foreign network ("***second sub-policy when Internet data service is provided through a roaming WWAN***"). SAMSUNG-1007, [0011], [0024], [0027], [0029]. In Rao, policies may be "specified hierarchically to account for multiple applications" and/or "multiple protocols that may be executed on [a] client [] at any point,"

demonstrating that hierarchical policy structures for adjusting the types of device functionality provided by Rao-Oestvall-Montemurro were conventional by the Critical Date. SAMSUNG-1005, [0182].

8. ***Claim 24***

[24] The wireless end-user device of claim 1, the first differential traffic control policy comprising first, second, and third sub-policies applicable respectively to Internet data service provided using the WWAN modem and three different network types from the network types consisting of 2G, 3G, 4G, home, and roaming.

157. As discussed for [23], a POSITA would have understood and found obvious configurations of Rao-Oestvall-Montemurro where an instance of the routing table with routing options for different types of networks (e.g., home network, foreign network). Montemurro identifies several types of WWAN, including "cellular technologies like GSM/GPRS EDGE, UTMS, HSPA, CDMA, WCDMA, etc." SAMSUNG-1007, [0003]. Given the types of examples identified, a POSITA would have understood and found obvious that various instances of the routing table may be configured to accommodate "***three different network types from the network types consisting of 2G, 3G, 4G, home, and roaming***." SAMSUNG-1007, [0022], [0029], [0037].

9. ***Claim 26***

[26] The wireless end-user device of claim 1, wherein the one or more network access conditions indicated via the API to the first end-user application

comprises information on whether a current connected WWAN is a roaming network or a non-roaming network.

158. *See* [24] above. Montemurro identifies several types of WWAN, including "cellular technologies like GSM/GPRS EDGE, UTMS, HSPA, CDMA, WCDMA, etc." SAMSUNG-1007, [0003]. Policies are "responsive to various factors," including "network roaming." *Id.*, [0029]. The rules engine "executes" the routing table to "ensure that data goes out to the most appropriate network (via respective network interface)" and "interacts with the connection API's to determine which interface would be best used to service a particular application." *Id.*, [0035]. Given such non-limiting disclosure and the types of examples identified, a POSITA would have understood and found obvious that an instance of the routing table includes "***information on whether a connected WWAN is a roaming network or a non-roaming network***." SAMSUNG-1007, [0022], [0029], [0037].

10. ***Claim 29***

[29] The wireless end-user device of claim 1, wherein the API instructs the first end-user particular application to transition to a different state.

159. As discussed for [1.8(a)], in Rao-Oestvall, an improved agent would have leveraged several types of APIs (including the recited "***API***") in regulating applications. SAMSUNG-1005, [0110], [0166], [0190], [0205]; SAMSUNG-1020, 3-4. As described for [1.8(a)] (Ground 1A), Oestvall incorporates by reference

Dive-Reclus, which teaches permission decisions regulating network access by third-party applications that use API calls. SAMSUNG-1006, [0020]; SAMSUNG-1026, 16:23-17:28, 20. A POSITA would have found it obvious that a permission decision denying network access results in "***transition to a different state***" (e.g., permitted network access, restricted network access), which is communicated to the application through a corresponding API ("***API instructs the first end-user application***"). SAMSUNG-1006, [0020]; SAMSUNG-1026, 16:23-17:28, 20.

160. Montemurro provides techniques that cause a user application to transition to a different state, e.g., "[s]ome access technology switches will result in IP address changes" so "an application using the connection needs to be aware of the IP address, the change may not be transparent and may need to be communicated to (or otherwise discoverable by) the application." *Id.*, [0048]. In another example, connection "differences are significant (e.g. between GSM/GPRS and WAN 802.11 technologies)" so "an application may need to tailor its behaviour to account for the new access technology in use" such as "[b]uffer sizes, re-transmission timers etc." that "may need to be changed." *Id.* A POSITA would have understood and found obvious scenarios where an application tailors its behavior (e.g., IP address changes, altered buffer sizes, and modified re-transmission timers) are examples of application transitions to different states. For example, Montemurro teaches that "applications can be developed and operated to

provide different usage models that may vary depending on the mode of operation that is available at runtime." SAMSUNG-1009, [0024]. The "[r]ules engine 206A configures the communication operations with a set of rules/policies that could include various factors such as radio access technology (e.g. for high/low bandwidth properties), cost, presence, time of day, location (e.g. geo-based policies, network roaming), destination IP address, application type, and Quality of Service (QoS) requirements, among others." *Id.*, [0029].

161. When an application state changes such that a network access condition adjusts the application's permission to access network resources, a POSITA would have understood and found obvious that for Rao-Oestvall-Montemurro, an API, e.g., the Java sockets API, provides instructions to the application to transition states relating to the network access condition ("***the API instructs the first end-user particular application to transition to a different state***"). As discussed for [1.8(a)], the Java Sockets API would have been one of several types of conventional APIs understood and found obvious by a POSITA to be within Rao's disclosure based on its contemplated API functionality. Such a configuration would have also supported Oestvall's disclosure that "[w]hen the untrusted application is brought to the foreground again, it is allowed to run again." SAMSUNG-1006, [0021], [0023]; SAMSUNG-1018, 15:44-55.

162. The use of APIs in Rao-Oestvall-Montemurro also coincides with the ’976 patent specification, where “[a] network API [that] can facilitate an application provider, central network/service provider, and/or a third party with access to communicate with the application to provide and/or request information (e.g., physical location of the application, network location of the application, network service usage information for the application, network busy state information provided to the application, and/or other criteria/measures).” SAMSUNG-1001, 73:47-54.

XII. [GROUND 1C] – RAO-OESTVALL-ARAUJO MAKES CLAIMS 12, 15, 21, AND 22 OBVIOUS

A. Combination of Rao, Oestvall, and Araujo

163. A POSITA would have found it obvious to modify Rao-Oestvall to include Araujo’s “request deflector component” to allow the Rao-Oestvall system to better “use the energy in a way that strikes a balance between providing functionality and maintaining longevity of the charge.” SAMSUNG-1011, [0001].

164. As discussed in Section XI.A, Rao-Oestvall provides functionality to control an application’s network access by intercepting network packets, determining the packet prioritization based on the application, and selectively communicating packets to the network based on the packet prioritization. In Rao, these prioritization operations can be performed by one or more “network drivers of a network stack 310” (e.g., by “customiz[ing], modif[ying] or adapt[ing]” the

network drivers "to provide a custom or modified portion of the network stack 310 in support of any of the techniques"). SAMSUNG-1005, [0100]. For example, the Rao-Oestvall system can include "[a] filter 322 [to] place, arrange, or coordinate network packets into queues 540a-540n in support of the priorities," and these "queues 540a-540n may be included in a network driver, such as an NDIS driver for the filter 322." *Id.*, [0143], [0180], [0191].

165. In implementing such functionality, a POSITA would have perceived opportunities for improving the interception capabilities already present in Rao to impart additional advantages, such as increasing energy efficiency. To this aspect, a POSITA would understood and found obvious that well-known monitoring capabilities may be useful to reduce power consumption and thereby increase the longevity of techniques provided by Rao-Oestvall while its device operates on battery power. *Id.* A POSITA would have thereby looked to Araujo's "request deflector component," which is "interposed" between each application and network driver, to selectively allow or block an application from transmitting data to the network. SAMSUNG-1011, [0050]. Incorporation of functionality of Araujo's "request deflector component" into Rao-Oestvall would have enabled assignment of a "status" to an application, use of that status to determine if allowing an application request "justifies the consumption of power under the circumstances that are present," and regulation (e.g., blocking, allowing) of the

request based on that determination. *Id.*, [0027]. Such a configuration would have thereby enjoyed the benefits of better using “energy in a way that strikes a balance between providing functionality and maintaining longevity of the charge.” *Id.*, [0001].

166. As an example of modifying Rao-Oestvall to incorporate Araujo’s teachings, a POSITA would have “interposed” Araujo’s “request deflector component” between applications and the network driver implementing Rao’s packet prioritization functionality (e.g., a network driver implementing the packet capture mechanism 364, filter 322, and queues 540a-540n). For example, a POSITA would have arranged Araujo’s “request deflector component” to process network packets after an application providing the network packets for transmission has otherwise been deemed by Oestvall’s window server component to be running in the foreground (and thereby having access to device resources). SAMSUNG-1006, [0025]. This configuration would have enabled further assessment of whether the application can access the network (e.g., in addition to considering whether an application has exceeded application-specific data limitations) in order to further enhance the efficiency of the Rao-Oestvall-Araujo combination.

167. A POSITA would have configured to the “request deflector component” to determine whether each of the applications has a “status [that]

justifies the consumption of power under the circumstances that are present," and selectively allow or block the network packets from proceeding to the network driver based on the determination. For example, upon determining that the application's status justifies the consumption of power, the "request deflector component" would allow the network packets to proceed to the network driver for prioritization (*see* step 1.5a below). Alternatively, upon determining that the application's status does not justify the consumption of power, the "request deflector component" would block the network packets from reaching the network driver, either permanently or temporarily (*see* step 1.5b below). *Id*. The "request deflector component" would have thereby provided an additional layer of control for regulating each of the applications' access to the network (e.g., to supplement the regulation techniques already present in Rao and Oestvall).

168. A POSITA would have had a reasonable expectation of success in combining Rao-Oestvall and Araujo, as discussed above. Incorporation of functionality of Araujo's "request deflector component" into Rao-Oestvall would have enabled assignment of a "status" to an application, use of that status to determine if allowing an application request "justifies the consumption of power under the circumstances that are present," and regulation (e.g., blocking, allowing) of the request based on that determination. SAMSUNG-1011, [0027]. Such a configuration would have enjoyed the benefits of better using "energy in a way that

strikes a balance between providing functionality and maintaining longevity of the charge." *Id.*, [0001]. Rao and Araujo also each discuss interception techniques, which would have led a POSITA to recognize that their respective disclosures address similar aspects relating to the benefits of regulating the operation of applications on a mobile device to improve device efficiency. SAMSUNG-1005, [0180], [1084]; SAMSUNG-1011, [0024], [0050].

169. Additionally, configuring Rao-Oestvall to leverage Araujo's teachings would have required only routine programming knowledge well within the skill of a POSITA prior to the earliest effective filing date. The change involved (1) combining prior art elements according to known methods to yield predictable results; and (2) use of a known technique to improve similar devices (methods, or products) in the same way. For example, Rao-Oestvall-Araujo would have provided a device that uses a set of policies to generally regulate applications, including policies used to prioritize network packet transmissions (as described in Rao), and evaluation of certain policies would have involved permitting or blocking an application's request (e.g., transmitting network packets) using a request deflector component (as described in Araujo). SAMSUNG-1005, [0100]; SAMSUNG-1011, [0024], [0050].

B. Analysis of Claims 21 and 22

1. *Claim 12*

[12] The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change the application of the first differential traffic control policy based on a power state of the device.

170. As discussed in Section IX.D, Araujo describes power management techniques for managing a "machine's power usage." SAMSUNG-1011, Abstract. This occurs through use of power management policies, which account for factors, such as "current power consumption, the amount of energy stored in a battery, predictions about future power usage, or any other factor." *Id.*, [0004]. Thus, in Rao-Oestvall-Araujo, power management is based on monitoring, for example, power consumption ("***power state***"). Rao-Oestvall-Araujo would have enabled changes to the way applications operate based on monitoring a power state, which a POSITA would have understood and found obvious involves, in some instances, adjusting a policy enforcement by Rao-Oestvall-Araujo for prioritization ("***dynamically change the application of the first differential traffic control policy***"). SAMSUNG-1011, [0031], [0046]. For example, "[a] power state change may be sought in order to turn on a device, or to raise the power state of a device, in order to allow the device to service a request from an application." SAMSUNG-1011, [0038]. In response, the Rao-Oestvall-Araujo device would respond by "block[ing] the request" and "program may receive an error code or result code."

Id., [0040]. One type of request is a network packet transmission request described in Rao, and a POSITA would have understood and found obvious that blockage of the request would have resulted in the Rao-Oestvall-Araujo device in selecting and/or applying a different policy for prioritization (e.g., selecting a policy that prioritizes packet transmissions of another application that would not necessitate a power state change). SAMSUNG-1005, [0182].

2. *Claim 15*

[15] The wireless end-user device of claim 1, wherein the one or more processors are further configured to dynamically change the application of the first differential traffic control policy based on power control state changes for one or more of the modems.

171. As discussed for [12], a POSITA would have understood and found obvious that Rao-Oestvall-Araujo adjusts policy enforcement for prioritization in certain circumstances involving a power state change. Araujo further describes "power may be controlled for devices" such as "disks, **network adapters**, processors, monitors." SAMSUNG-1011, [0018]. A POSITA would have understood and found obvious that a modem is an example of network adapter, and thus, Rao-Oestvall-Araujo would have provided power management for "***one or more modems***." A POSITA would have therefore understood and found obvious that, in some instances, Rao-Oestvall-Araujo adjusts a policy enforcement by Rao-Oestvall-Araujo for prioritization based on a power state change for a modem ("***dynamically change the application of the first differential traffic control***

policy”). SAMSUNG-1011, [0031], [0046]. For example, POSITA would have understood that a modem is a type of network adapter that serves the purpose of enabling communication between a computer and a network.

172. A POSITA would have further found obvious that the monitored power state includes “***power control state changes***,” which would then be used as a basis for a configuration change. For example, Cole offers examples of “communication load monitoring and deferred action functions” that a POSITA would have understood and found obvious to be improved by policy application by Rao-Oestvall-Araujo. SAMSUNG-1009, [0088]-[0091]. Cole further recognizes that “[a] lengthy transfer [that] is conducted using [a] WWAN modem 230 (e.g., a 3G channel)” “consumes significant battery power” and, in response, the connection manager “asks the user to find a better connection.” SAMSUNG-1009, [0088]. From this example, a POSITA would have recognized that, since modem usage impacts power consumption, changes in a connectivity state of a modem represent changes in the modem’s power control state.

3. *Claim 21*

[21] The wireless end-user device of claim 20, wherein the API responds to an intercepted request by the first end-user application by emulating network messaging.

173. As discussed for [1.8(a)], Rao-Oestvall-Araujo would have provided an improved agent that uses one or more APIs as a “means” or “mechanism” to

provide communications relating to prioritization." SAMSUNG-1005, [0110], [0166], [0190], [0205]. In Rao, communications related to prioritization may be accomplished using any "form or interface known to those ordinarily skilled in the art." *Id.*, [0190]. Based on these non-limiting disclosures in Rao, a POSITA would have found obvious that in incorporating Araujo's "request deflector component" into Rao-Oestvall (as discussed in Section XIV.A), certain exemplary configurations involve the "request deflector component" being implemented to provide communications functionality as an API. In such configurations of Rao-Oestvall-Araujo, the "request deflector component" renders the "***API***" recited in claim 21 obvious since the "request deflector component" in Rao-Oestvall-Araujo would have provided the functionality recited in the claim (e.g., emulating network messaging) as being performed by the API, as further addressed below.

174. Indeed, APIs that were configured to provide emulating network messaging functionality between applications and drivers were well-known as of the Critical Date. For example, Sng (U.S. Pat. No. 8,413,172) describes a "socket API 220" with an emulation module for "socket API call emulation." SAMSUNG-1015, Abstract, FIG. 2. Like Araujo's "request deflector component" being "interposed" between applications and drivers, Sng's socket API 220 is similarly interposed between applications (e.g., application 210) and drivers (e.g., non-networked I/O device driver 240, networked I/O device driver 250). *See id.*, 3:46-

5:10; *see also* SAMSUNG-1011, [0050]. As another example, as discussed for [1.8(a)], Flinn described an "API" that "offers both blocking and event-based interfaces…" SAMSUNG-1016, 1. Flinn further indicates the existence of "API features to the normal socket interface[,]" including application regulation mechanisms, such as "block[ing] [a] message until the network is available, with an optional timeout," which is "more useful to threaded applications." *Id.*, 3. These disclosures relate to interception and blocking (concepts similarly contemplated in Rao and Araujo) and would have been pertinent to in implementing Rao-Oestvall-Araujo, as discussed in Section XIV.A. SAMSUNG-1005, [0143], [0100], [0180], [0191]; SAMSUNG-1011, [0001], [0027], [0050]. Moreover, the use of APIs to regulate network communications within a layered computing architecture was similarly well-known before the Critical Date. SAMSUNG-1017, 11. These disclosures similarly coincide with relevant disclosure in the '976 patent relating to APIs that provide emulating network messaging. *See, e.g.*, SAMSUNG-1001, 91:25-67 ("emulating network API can intercept, modify, block, remove, and/or replace network socket application interface massages and/or EtherType messages").

175. Further as discussed in Section XIV.A, in Rao-Oestvall-Araujo, "if the power state change is not allowable under [a] policy," the device can "block the request" and "notif[y] [the program] that the request will not be processed."

SAMSUNG-1011, [0038], [0041]. Further, "[t]he program may also be notified that the reason for the request is that the device is off[,]" e.g., "the program may receive an error code or result code indicating that the request calls for a device that is not turned on." *Id.*; *see also id.*, [0017] ("Thus, a program could be notified that a request to use a device is not being put through to the device because the request would be contrary to power-usage policy."). Based on these disclosures, a POSITA would have understood and found obvious that the Rao-Oestvall-Araujo would have responded to an intercepted request by an application by notifying the application that the request will not the processed and/or transmitting an error code or result code to the application ("***respond[] to an intercepted request by the first end-user application by emulating network messaging***"). In doing so, the combined device would have provided the application have with a greater degree of information regarding its attempt to access a network, as taught by Araujo.

176. Moreover, Araujo's use of an "error code or result code" is consistent with the '976 patent specification's disclosure of an "emulated network API" that blocks an application's connection attempt and sends "a message…back to the application" regarding the blocking, such as a message that "the application will understand and can interpret to indicate that the network access attempt was not allowed/blocked, that the network is not available, and/or to try again later for the requested network access." SAMSUNG-1001, 91:25-49.

4. ***Claim 22***

[22] The wireless end-user device of claim 21, wherein emulating network messaging comprises responding to a network request from the first end-user application by blocking the request from passing to a network stack and returning to the first end-user application a message indicating the network request was not successful.

177. As discussed for [21], a POSITA would have configured Rao-Oestvall-Araujo to respond to an intercepted request by an application by notifying the application that the request will not the processed and/or transmitting an error code or result code to the application ("***emulating network messaging***"). As discussed in Section XIV.A, Rao-Oestvall-Araujo would have incorporated Araujo's "request deflector component" to "intercept[] requests and respond[] to the requests based on power management considerations before the requests reach a device driver." SAMSUNG-1011, [0024], [0050].

178. A POSITA would have also understood and found obvious to configure Rao-Oestvall-Araujo such that, in blocking a request from reaching the network driver, the request is prevented from being provided to Rao's "network stack" (which includes "one or more network drivers supporting the one or more layers" of the network stack) ("***responding to a network request from the end-user application by blocking the request from passing to a network stack***"). SAMSUNG-1005, [0100].

179. In Rao-Oestvall-Araujo, "if the power state change is not allowable under the policy," the device can "block the request" and "notif[y] [the program] that the request will not be processed." SAMSUNG-1011, [0038], [0041]. Further, "[t]he program may also be notified that the reason for the request is that the device is off[,]" e.g., "the program may receive an error code or result code indicating that the request calls for a device that is not turned on" ("***...and returning to the particular application a message indicating the network request was not successful***"). *Id.*; *see also id.*, [0017] ("Thus, a program could be notified that a request to use a device is not being put through to the device because the request would be contrary to power-usage policy.").

XIII. CONCLUSION

180. The findings and opinions set forth in this declaration are based on my work and examinations to date.

181. I may continue my examinations. I may also receive additional documentation and other factual evidence over the course of this IPR that will allow me to supplement and/or refine my opinions. I reserve the right to add to, alter, or delete my opinions and my declaration upon discovery of any additional information. I reserve the right to make such changes as may be deemed necessary.

182. In signing this declaration, I recognize that the declaration will be filed as evidence in an IPR before the PTAB. I also recognize that I may be subject

to cross-examination in the case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

183. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

APPENDIX A

KEVIN RAYMOND BOYCE BUTLER

Professor		Address :	E301 CSE Building
Department of Computer & Information Science and Engineering			PO Box 116120
University of Florida			Gainesville FL 32611
email:	butler@ufl.edu	Phone:	+1 (352) 294-2090
URL:	http://www.kevinbutler.org	Fax:	+1 (352) 392-1220

Current Academic Appointment

Professor, Department of Computer and Information Science and Engineering, University of Florida, Aug. 2021 - *present*
Director, Florida Institute for Cybersecurity Research, University of Florida, Aug. 2022 - *present*

Educational Background

Ph.D. in Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, August 2010 (Dissertation Title: *Leveraging Emerging Storage Functionality for New Security Services*; Advisor: Dr. Patrick McDaniel)
M.S. in Electrical Engineering, Columbia University, New York, NY, USA, May 2003 (Advisor: Dr. Henning Schulzrinne)
B.Sc. in Electrical Engineering, Queen's University, Kingston, ON, Canada, May 1999

Honors & Awards

Best Paper Award, ACM HotStorage, 2023.
Meta Research Award, Meta Research Labs, 2022-2023.
Best Paper Finalist, IEEE European Symposium on Security and Privacy, 2022.
University Term Professor, University of Florida, 2021-2024.
Best Paper Nominee, IEEE Conference on Virtual Reality, 2021.
Doctoral Dissertation Advisor/Mentoring Award, Herbert Wertheim College of Engineering, University of Florida, 2019.
Distinguished Poster Award, ACM CODASPY, 2019.
Arnold and Lisa Goldberg Rising Star Endowed Professorship, University of Florida, 2018-2024 *(relinquished in 2021 upon promotion to Professor)*.
University Term Professor, University of Florida, 2018-2021.
Recognition of Service Award, Association for Computing Machinery, 2018.
Research Promotion Initiative Award, University of Florida, 2018.
Senior Member, Association for Computing Machinery, 2018.
International Educator of the Year, Herbert Wertheim College of Engineering, University of Florida, 2017.
Senior Member, IEEE, 2017.
Outstanding Community Service Award, IEEE Technical Committee on Security and Privacy, 2017.
Rising to National Preeminence Hire, University of Florida, 2014.

Best Teacher Award, Dept. of Computer and Information Science, University of Oregon, 2013.
CAREER Award, National Science Foundation, 2013.
Alumni Association Dissertation Award, Pennsylvania State University, 2010.
Symantec Intern Project Showcase Winner, Symantec Corp, 2009.
Graduate Research Assistant Award, Computer Science and Engineering Department, Pennsylvania State University, 2009.
Symantec Graduate Fellowship, Symantec Research Labs, 2009-2010.
Special Award of Meritous Service, Third International Conference on Information Systems Security, December 2007.
University Graduate Fellowship, Pennsylvania State University, 2006.
C. Norwood Wherry Memorial Graduate Fellowship, Pennsylvania State University, 2004.

Expert Witness Experience

During the course of my expert witness consulting engagments, I have written numerous expert reports, given six depositions, and have testified four times across two jury trials, with regards to both patent infringement and invalidity.

Testfiying Expert, *Headwater Research LLC v. Samsung America Inc., No. 2-22-cv-00422, 2-22-cv-00467, 2:23-cv-00103 (E.D. Texas)*, retained by Fish and Richardson, representing defendent, April 2023 - present.

Testifying Expert, *Webroot, Inc. et al. v. Trend Micro Inc., No. 6:22-cv-00239-ADA-DTG (W.D. Texas)*, retained by Paul Hastings LLP and White & Case LLP, regarding intrusion detection devices, representing defendant. July 2022-present.

Consulting Expert, *Department of Justice, Antitrust Division, defendant confidential*, retained by USDOJ, regarding mobile devices. June 2022-June 2023.

Testifying Expert, *Research in Motion Limited ats Glen Snowball (File No. 13-57203CP), Blackberry Limited ats Michael Blackette (File No. 500-06-000583-118)*, retained by Torys LLP, regarding the Blackberry network, representing defendent. March 2021-present.

Testifying Expert, *IOENGINE LLC vs Roku Inc.* regarding portable devices, engaged by plaintiff in patent infringement case, October 2021-present.

Testifying Expert, *Finjian, Inc. v. Juniper Networks, Inc. (3:17-cv-0569-WHA, District Court, N.D. California)*, retained by Irell and Manella LLP, regarding intrusion detection systems, representing defendant. June 2019-August 2019.

Testifying Expert, *Ingenico Inc v. IOENGINE LLC (1:18-cv-00826, District Court, D. Delaware)*, retained by Dechert LLP, regarding secure portable devices, representing defendant. October 2018-December 2022.

Testifying Expert, *IOENGINE LLC v. Imation Corp. (1:14-cv-01572, District Court, D. Delaware)*, retained by Simpson Thacher & Bartlett LLP, regarding secure portable storage devices, representing plaintiff. March 2015-February 2017.

Testifying Expert, *IOENGINE LLC v. Interactive Media Corp. (1:14-cv-01571, District Court, D. Delaware)*, retained by Simpson Thacher & Bartlett LLP, regarding secure portable storage devices, representing plaintiff. March 2015-January 2017.

Consulting Expert, *Vir2us, Inc.*, retained by Bunsow, De Mory, Smith, and Allison LLP, regarding virtualization and antivirus software. December 2014 - April 2015

Consulting Expert, *Envosys v. AT&T*, retained by Baker Botts, regarding location services in mo-

bile devices, representing defendant. October 2013-December 2013.

Research Support ($36.7M total, $9.34M investigator share)

Major Peer-Reviewed Grants ($36.0M total, $10.8M as PI, $9.00M investigator share)

- **PI**, *NSF CNS-2206950, "Collaborative Research: SaTC: Frontiers: Securing the Future of Computing for Marginalized and Vulnerable Populations"*, National Science Foundation, $7,500,000 ($2,630,872 investigator share), 10/1/2022-9/30/2027.
- **Site PI**, *NSF CNS-2054911, "Collaborative Research: SaTC: CORE: Medium: Enabling Practically Secure Cellular Infrastructure"*, National Science Foundation, $1,199,985 ($598,019 investigator share), 1/1/2022-12/31/2024.
- **co-PI**, *NSF CNS-2055123, "SaTC: CORE: Medium: Countering Surveillanceware Using Deception-Based Generative Models and Systems Mechanisms"*, National Science Foundation, $1,199,997 ($618,531 investigator share), 1/1/2021-12/31/2024.
- **co-PI**, *ONR N00014-20-1-2205, "Reconstructing Human Physiological Features from Audio Samples"*, Office of Naval Research, $700,000 ($333,232 investigator share), 6/11/2021-6/10/2024.
- **co-PI**, *DHS 70RSAT20CB0000017, "Deploying Defenses for Cellular Networks Using the AWARE Testbed"*, DHS, $3,122,033 ($657,536 investigator share), 9/30/2020-9/29/2024.
- **PI**, *ONR BAA-N00014-19-S-B001 Grant 12941701, "Mobile Interface Security Analysis"*, Office of Naval Research, $700,000 ($376,242 investigator share), 1/1/2020-12/31/2022.
- **PI**. *AFOSR AACOE, "Interpretable Security Reference Monitor for Deep Networks"*, Air Force Office of Scientific Research, $185,000 ($185,000 investigator share), 12/1/2019-8/31/2021.
- **co-PI**, *ONR DOD-19-STTR, "ArtusProtocol"*, Office of Naval Research, $800,000 ($400,000 investigator share), 8/1/2019-7/31/2021.
- **co-PI**, *AFOSR FA8650-19-1-1741, "University Center of Excellence: CYAN: Enabling Cyber Defense in Analog and Mixed Signal Domain"*, Air Force Office of Scientific Reesarch, $5,000,000 ($300,000 investigator share), 10/1/2019-9/30/2024. Selected for funding by AFOSR on 5/24/2019.
- **co-PI**, *AFRL-FA9550-19-1-0169, "AFOSR University Center of Excellence in Assured Autonomy in Contested Environments (AACOE)"*, Air Force Office of Scientific Research and Air Force Reesarch Labs, $5,999,515 ($389,999 investigator share), 3/1/2019-2/28/2024.
- **co-PI**, *DARPA HR00118S0052, "RACE: Resilient Communications for Everyone"*, Defense Advanced Research Projects Agency, $1,133,856 ($382,698 investigator share), 3/1/2019-2/28/2023. Selected for funding by DARPA on 11/20/2018.
- **PI**, *NSF/SRC CNS-1815883, "SaTC: STARSS: Small: Domain Informed Techniques for Detecting and Defending Against Malicious Firmware"*, National Science Foundation, $499,990 ($250,000 investigator share), 11/01/2018-10/31/2021.

- **co-PI**, *NSF CNS-1662976, "Collaborative Research: SURPASS: NSF SFS Unique Scholarship Program in Hardware and Systems Security"*, National Science Foundation, $2,508,541 ($35,408 investigator share), 01/01/2017-12/31/2021.
- **co-PI**, *NSF CNS-1562485, "TWC: Medium: Digital Healthcare-Associated Infection: Measurement, Defense and Prevention in a Modern Digital Healthcare Ecosystem"*, National Science Foundation, $1,200,000 ($387,931 investigator share), 06/01/2016-05/31/2020.
- **PI**, *"Developing Research Capability in Cyber-Physical Systems at the University of Florida"*, Defense University Research Instrumentation Program (DURIP), Army Research Office, $199,919 ($100,000 investigator share), 09/01/2015-08/31/2016.
- **PI**, *NSF CNS-1445983/1540216, "EAGER: Collaborative: Secure and Efficient Data Provenance"*, National Science Foundation, $205,000 *($110,000 investigator share)*, 10/01/2014-03/31/2016.
- **PI**, *NSF CNS 1254198/1540217, "CAREER: Securing Critical Infrastructure with Autonomously Secure Storage"*, National Science Foundation, $400,000, 04/01/2013-03/31/2018.
- **PI**, *NSF CNS 1118046/154028, "TC:Small:Protection Mechanisms for Portable Storage"*, National Science Foundation, $515,530, 09/01/2011-08/31/2016.
- **co-PI**, *"GAANN Program on Computer Systems Security"*, US Department of Education, $1,476,931 *($184,616 investigator share)*, 08/16/2015-08/15/2018.
- **co-PI**, *DARPA BAA 10-81, "Characterizing and Implementing Efficient Primitives for Privacy-Preserving Computation"*, Defense Advanced Research Projects Agency and Air Force Research Labs, $550,000 *($262,375 investigator share)*, 05/01/2011-01/31/2015.

Industry and Other Support

- **co-PI**, *"Mitigating Threat of Re-Identification from Eye-Tracking Data"*, Meta Privacy-Enhancing Technology Award, $100,000 (*($49,000 investigator share)), 9/1/2022-8/31/2023.*
- **co-PI**, "Center for Aerospace Resilience"*, Florida Department of Education, $875,000* ($126,214 investigator share)*, 7/1/2020-7/31/2021.*
- **PI**, "Secure Enclave Computing"*, Royal Bank of Canada, $87,347, 11/01/2019-01/01/2021.*
- **PI**, NSF 1823067, "Travel Grant Support for ACM WiSec"*, National Science Foundation, $9,000, 05/27/2018-05/26/2019.*
- **Co-PI**, "Formal Analysis of SGX Platform Software"*, Intel Corporation, $50,000* ($25,000 investigator share)*, 01/01/2018-12/31/2018.*
- **PI**, "Smartphones and Mobile money: Analysis and Recommendations for Security"*, GSMA Mobile For Development Foundation, $28,500* ($13,500 investigator share)*, 12/01/2017-03/31/2018.*
- **PI**, "Provenance-Based Enforcement Mechanisms"*, MIT Lincoln Laboratory, $137,000, 11/01/2013-10/31/2016.*

- **PI**, “Securing Storage for Insider Threat Mitigation”, *Florida Cyber Consortium Seed Grant, $40,000* ($20,000 investigator share), *2015.*
- **co-PI**, “Resilience in BGPSec”, *Battelle, $180,000* $80,000 investigator share, *02/01/2012-08/31/2013.*
- **co-PI**, “A Cyber-Security Center of Excellence for Oregon”, *Oregon Engineering, Technology, and Industry Council, $180,000* ($60,000 investigator share), *06/01/2014-05/31/2015.*
- **co-PI**, “I3: An Interdisciplinary Approach to Internet Privacy”, *University of Oregon Research, Innovation and Graduate Education, $50,000, 04/10/2014-03/31/2015.*
- **PI**, NSF CNS 1329307, “Oregon Security Day”, *National Science Foundation, $8,000, 03/01/2013-04/30/2014.*
- **Recipient**, “USB Fingerprinting”, *Ellisys, equipment donation, $8,000, 2011.*
- **Recipient**, “Project HAWAII”, *Microsoft Research, equipment donation, $1,000, 2011.*

Publications (4986 citations [Google Scholar, July 2023], h-index=39, i10-index=73)

Book Chapters

1. Adam Bates, Devin Pohly, and Kevin R. B. Butler. “Secure and Trustworthy Provenance Collection for Digital Forensics.” In C. Wang, R. M. Gerges, Y. Guan, and S. K. Kasera, eds.,*Digital Fingerprinting* (pp. 141–176). New York: Springer-Verlag, 2016.
2. Kevin Butler, William Enck, Patrick Traynor, Jennifer Plasterr, and Patrick McDaniel. “Privacy Preserving Web-Based Email”. *Algorithms, Architectures and Information Systems Security*, Statistical Science and Interdisciplinary Research. World Scientific Computing, November 2008.

Journal Publications

3. Brendan David-John, Kevin Butler, and Eakta Jain. “Privacy-preserving Datasets of Eye-tracking Samples with Applications in XR.” *IEEE Transactions on Visualization and Computer Graphics*, January 2023. 11 pages. *Selected for presentation at IEEE VR 2023 conference.*
4. Weidong Zhu and Kevin Butler. “NASA: NVM-Assisted Secure Deletion for Flash Memory.” *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, July 2022 (early access). Accepted for presentation at the International Conference on Embedded Software (EMSOFT) 2022.
5. Tuba Yavuz, Farhaan Fowze, Grant Hernandez, Ken (Yihang) Bai, Kevin Butler, and Dave (Jing) Tian. “ENCIDER: Detecting Timing and Cache Side Channels in SGX Enclaves and Cryptograpihc APIs.” *IEEE Transactions on Dependable and Secure Computing*, March 2022 (early access). 18 pages.
6. Brendan David-John, Diane Hosfelt, Kevin Butler, and Eakta Jain. “A Privacy-Preserving Approach to Streaming Eye-Tracking Data.” *IEEE Transactions on Visualization and Computer Graphics*, March 2021 (early access). 11 pages. *Best paper nominee at IEEE VR 2021 conference.*
7. Farhaan Fowze, Grant Hernandez, Dave (Jing) Tian, Kevin Butler, and Tuba Yavuz. “ProXray: Pro-

tocol Model Learning and Guided Firmware Analysis." *IEEE Transactions on Software Engineering*, September 2019.

8. Grant Hernandez, Dave (Jing) Tian, Farhaan Fowze, Tuba Yavuz, Patrick Traynor, and Kevin Butler. "Towards Automated Firmware Analysis in the IoT Era." *IEEE Security and Privacy*, 17(5), pg. 38-46, Sept.-Oct. 2019.

9. Joseph Choi and Kevin Butler. "Secure Multiparty Computation and Trusted Hardware: Examining Adoption Challenges and Opportunities". *Security and Communication Networks*, vol 2019, Article ID 1368905, 28 pages, April 2019.

10. Benjamin Mood and Kevin Butler. "PAL: A System for Optimizing Secure Function Evaluation in Mobile Devices". *Journal of Information Security and Applications,* 40(2018), pg. 78-91, March 2018.

11. Bradley Reaves, Luis Vargas, Nolen Scaife, Dave (Jing) Tian, Logan Blue, Patrick Traynor, and Kevin Butler. "Characterizing the Security of the SMS Ecosystem with Public Gateways". *ACM Transactions on Privacy and Security*, 22(1), Article 2, January 2018.

12. Nolen Scaife, Patrick Traynor, and Kevin Butler. "Making Sense of the Ransomware Mess (and planning a sensible path forward)". *IEEE Potentials*, 36(6), pg. 28-31, Nov/Dec. 2017.

13. Dave (Jing) Tian, Kevin R. B. Butler, Joseph Choi, Patrick D. McDaniel, and Padma Krishnaswamy. "Securing ARP/NDP From the Ground Up." *IEEE Transactions on Information Forensics and Security*, 12(9), pg. 2131-2143, September 2017.

14. Adam Bates, Dave (Jing) Tian, Grant Hernandez, Thomas Moyer, Kevin R. B. Butler, and Trent Jaeger. "Taming the Costs of Trustworthy Provenance through Policy Reduction." *ACM Transactions on Internet Technology*, 17(4), Article 34, September 2017.

15. Bradley Reaves, Jasmine Bowers, Nolen Scaife, Adam Bates, Arnav Bhartiya, Patrick Traynor, and Kevin Butler. "Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications". *ACM Transactions on Privacy and Security*, 20(3), Article 11, August 2017.

16. Bradley Reaves, Jasmine Bowers, Sigmund Albert Gorski III, Rahul Bobate, Raymond Cho, Hiranava Sas, Sharique Hussain, Hamza Karachiwala, Nolen Scaife, Byron Wright, Kevin Butler, William Enck, and Patrick Traynor. "*droid: Assessment and Evaluation of Android Application Analysis Tools". *ACM Computing Surveys*, 49(3), Article 55, November 2016.

17. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. "Outsourcing Secure Two-Party Computation as a Black Box". *Security and Communication Networks*, 9(14), pg. 2261-2275, September 2016.

18. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. "Secure Outsourced Garbled Circuit Evaluation for Mobile Devices." *Journal of Computer Security*, 24(2), pg. 137-180, 2016.

19. Adam Bates, Kevin Butler, Micah Sherr, Clay Shields, Patrick Traynor, and Dan Wallach. "Accountable Wiretapping -or- I Know That You Can Hear Me Now". *Journal of Computer Security*, 23 (2015), pg. 167-195, 2015.

20. Adam Bates, Benjamin Mood, Joe Pletcher, Hannah Pruse, Masoud Valafar, and Kevin Butler. "On Detecting Co-Resident Cloud Instances Using Network Flow Watermarking Techniques". *International Journal of Information Security*, 13(2), pg. 171-189, April 2014.

21. Thomas Moyer, Kevin Butler, Joshua Schiffman, Patrick McDaniel, and Trent Jaeger. "Scalable Web

Content Attestation". *IEEE Transactions on Computers*, 61((5), pg. 686-699, May 2012.

22. Kevin Butler, Stephen McLaughlin, Thomas Moyer, and Patrick McDaniel. "New Security Architectures Based on Emerging Disk Functionality". *IEEE Security and Privacy*, 8(5), pg. 34-31, Sept./Oct. 2010.

23. Kevin Butler, Toni Farley, Patrick McDaniel, and Jennifer Rexford. "A Survey of BGP Security Issues and Solutions". *Proceedings of the IEEE*, 98(1), pg. 100-122, January 2010.

24. Patrick Traynor, Kevin Butler, William Enck, Kevin Borders, and Patrick McDaniel. "*malnets:* Large-Scale Malicious Networks via Compromised Wireless Access Points". Journal of Security and Communication Networks (SCN). 2009.

25. Kevin Butler, Sunam Ryu, Patrick Traynor, and Patrick McDaniel. "Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems". *IEEE Transactions on Parallel and Distributed Systems*, 20(12), pg. 1803-1815, December 2009.

26. Patrick McDaniel, William Aiello, Kevin Butler, and John Ioannidis, Origin Authentication in Interdomain Routing. *Computer Networks*, 50(16), pg. 2953-2980, 14 November 2006.

Conference Publications

Top-4 Security Conferences

27. Daniel Olszewski, Allison Lu, Carson Stillman, Kevin Warren, Cole Kitroser, Alejandro Pascual, Divyajyoti, Kevin Butler, and Patrick Traynor. ""Get in Researchers; We're Measuring Reproducibility": A Reproducibility Study of machine Learning Papers in Tier 1 Security Conferences". 30th ACM Conference on Computer and Communications Security (CCS'23), Copenhagen, Denmark, November 2023. *Acceptance rate TBD.*

28. Kyungtae Kim, Sungwoo Kim, Kevin Butler, Antonio Bianchi, and Dave (Jing) Tian. "Fuzz The Power: Dual-role State Guided Black-box Fuzzing for USB Power Delivery". *32nd USENIX Security Symposium (Security'23)*, Anaheim, CA, USA, August 2023. *Acceptance rate TBD.*

29. Yazhou Tu, Liqun Shen, Md Imran Hossen, Sara Rampazzi, Kevin Butler, and Xiali Hei. "Auditory Eyesight: Demystifying μs-Precision Keystroke Tracking Attacks on Unconstrained Keyboard Inputs". *32nd USENIX Security Symposium (Security'23)*, Anaheim, CA, USA, August 2023. *Acceptance rate TBD.*

30. Yan Long, Pirouz Naghavi, Blas Kojusner, Kevin Butler, Sara Rampazzi, and Kevin Fu. "Side eye: Characterizing the Limits of POV Acoustic Eavesdropping from Smartphone Cameras with Rolling Shutters and Movable Lenses". *44th IEEE Symposium on Security and Privacy (Oakland'23)*, San Francisco, CA, USA, May 2023. *Acceptance rate TBD.*

31. Tyler Tucker, Hunter Searle, Kevin Butler, and Patrick Traynor. "Blue's Clues: Practical Discovery of Non-Discoverable Bluetooth Devices". *44th IEEE Symposium on Security and Privacy (Oakland'23)*, San Francisco, CA, USA, May 2023. *Acceptance rate TBD.*

32. Logan Blue, Kevin Warren, Hadi Abdullah, Cassidy Gibson, Luis Vargas, Jessica O'Dell, Kevin Butler, and Patrick Traynor. "Who Are You (I Really Wanna Know)?" *31st USENIX Security Symposium (Security'22)*, Boston, MA, USA, Aug 2022. *Acceptance rate: 18.1%.*

33. Kyungtae Kim, Taegyu Kim, Ertza Warriach, Byoungyoung Lee, Kevin Butler, Antonio Bianchi,

and Dave (Jing) Tian. "FuzzUSB: Hybrid Stateful Fuzzing of USB Gadget Stacks." *43rd IEEE Symposium on Security and Privacy (Oakland'22)*, San Francisco, CA, USA, May 2022. *Acceptance rate: 14.5%.*

34. Grant Hernandez, Marius Muench, Dominik Maier, Alyssa Milburn, Shinjo Park, Tobias Scharnowski, Tyler Tucker, Patrick Traynor, and Kevin Butler. "FirmWire: Transparent Dynamic Analysis for Cellular Baseband Firmware." *2022 ISOC Network and Distributed System Security Symposium (NDSS'22)*, San Diego, CA, USA, April 2022. *Acceptance rate: 16.2%.*

35. Grant Hernandez, Dave (Jing) Tian, Anurag Yadav, Byron J. Williams, and Kevin Butler. "BigMAC: Fine-Grained Policy Analysis of Android Firmware." *29th USENIX Security Symposium (Security'20)*, Boston, MA, USA, August 2020. (*Acceptance rate: 16.1%.*)

36. Dave (Jing) Tian, Grant Hernandez, Joseph Choi, Vanessa Frost, Peter Johnson, and Kevin Butler. "LBM: A Security Framework for Peripherals within the Linux Kernel." *40th IEEE Symposium on Security and Privacy (Oakland'19)*, San Francisco, CA, USA, May 2019. (*Acceptance rate=12.0%.*)

37. Luis Vargas, Logan Blue, Vanessa Frost, Christopher Patton, Nolen Scaife, Kevin Butler, and Patrick Traynor. "Digital Healthcare-Associated Infection Analysis of a Major Multi-Campus Hospital System." *26th ISOC Network and Distributed System Security Symposium (NDSS'19)*, San Diego, CA, USA, February 2019. *(Acceptance rate=17.1%)*

38. Hadi Abdullah, Washington Garcia, Christian Peeters, Patrick Traynor, Kevin Butler, and Joseph Wilson. "Practical Hidden Voice Attacks against Speech and Speaker Recognition Systems." *26th ISOC Network and Distributed System Security Symposium (NDSS'19)*, San Diego, CA, USA, February 2019. *(Acceptance rate=17.1%)*

39. Luis Vargas, Gyan Hazarika, Rachel Culpepper, Kevin Butler, Thomas Shrimpton, Doug Szjada, and Patrick Traynor. "Mitigating Risk while Complying with Data Retention Laws." *25th ACM Conference on Computer and Communications Security (CCS'18)*, Toronto, ON, Canada, October 2018. *(Acceptance rate=17.0%)*

40. Dave (Jing) Tian, Grant Hernandez, Joseph Choi, Vanessa Frost, Christie Ruales, Patrick Traynor, Hayawardh Vijaykumar, Lee Harrison, Amir Rahmati, Mike Grace, and Kevin Butler. "ATtention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem." *27th USENIX Security Symposium (Security'18)*, Baltimore, MD, USA, August 2018. *(Acceptance rate=19.1%)*

41. Dave (Jing) Tian, Nolen Scaife, Deepak Kumar, Michael Bailey, Adam Bates, and Kevin Butler. "SoK: "Plug & Pray" Today – Understanding USB Insecurity in Versions 1 through C." *2018 IEEE Symposium on Security and Privacy (Oakland'18)*, San Francisco, CA, USA, May 2018. *Nominated for Distinguished Paper Award. (Acceptance rate=11.5%)*

42. Christian Peeters, Hadi Abdullah, Nolen Scaife, Jasmine Bowers, Patrick Traynor, Bradley Reaves, and Kevin Butler. "Sonar: Detecting SS7 Redirection Attacks Via Call Audio-Based Distance Bounding." *2018 IEEE Symposium on Security and Privacy (Oakland'18)*, San Francisco, CA, USA, May 2018. *(Acceptance rate=11.5%)*

43. Grant Hernandez, Farhaan Fowze, Dave (Jing) Tian, Tuba Yavuz, and Kevin Butler. "FirmUSB: Vetting USB Device Firmware using Domain Informed Symbolic Execution." *24th ACM Conference on Computer and Communications Security (CCS'17)*, Dallas, TX, USA October 2017. *(Acceptance rate=18.1%.)*

44. Dave (Jing) Tian, Adam Bates, Kevin Butler, and Raju Rangaswami. "ProvUSB: Block-level Provenance-Based Data Protection for USB Storage Devices." *23rd ACM Conference on Computer and Communications Security (CCS'16)*, Vienna, Austria, October 2016. *(Acceptance rate=16.5%.)*
45. Dave (Jing) Tian, Nolen Scaife, Adam Bates, Kevin Butler, and Patrick Traynor. "Making USB Great Again with USBFILTER". *25th USENIX Security Symposium (Security'16)*, Austin, TX, USA, August 2016. *(Acceptance rate=15.5%.)*
46. Bradley Reaves, Dave Tian, Nolen Scaife, Logan Blue, Patrick Traynor, and Kevin Butler. "Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways". *2016 IEEE Symposium on Security and Privacy (Oakland'16)*, San Jose, CA, USA, May 2016. *(Acceptance rate=13.3%.)*
47. Adam Bates, Dave Tian, Kevin Butler, and Thomas Moyer. "Trustworthy Whole-System Provenance for the Linux Kernel". *24th USENIX Security Symposium (Security'15)*, Washington, DC, USA, August 2015. *(Acceptance rate=15.7%)*
48. Bradley Reaves, Nolen Scaife, Adam Bates, Patrick Traynor, and Kevin Butler. "Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World". *24th USENIX Security Symposium (Security'15)*, Washington, DC, USA, August 2015. *(Acceptance rate=15.7%)*
49. Benjamin Mood, Debayan Gupta, Kevin Butler, and Joan Feigenbaum. "Reuse It Or Lose It: More Efficient Secure Computation Through Reuse of Encrypted Values". *21st ACM Conference on Computer and Communications Security (CCS'14)*, Scottsdale, AZ, USA, November 2014. *(Acceptance rate=19%)*
50. Adam Bates, Joe Pletcher, Tyler Nichols, Braden Hollembaek, Dave Tian, Abdulrahman Alkhelaifi, and Kevin Butler. "Securing SSL Certificate Verification through Dynamic Linking". *21st ACM Conference on Computer and Communications Security (CCS'14)*, Scottsdale, AZ, USA, November 2014. *(Acceptance rate=19%)*
51. Adam Bates, Ryan Leonard, Hannah Pruse, Daniel Lowd, and Kevin Butler. "Leveraging USB to Establish Host Identity Using Commodity Devices." *21st ISOC Network and Distributed System Security Symposium (NDSS'14)*, San Diego, CA, USA, February 2014. *(Acceptance rate=18.6%)*
52. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. "Secure Outsourced Garbled Circuit Evaluation for Mobile Devices". *22nd USENIX Security Symposium (Security'13)*, Washington, DC, USA, August 2013. *(Acceptance rate=16.2%.)*
53. Benjamin Kreuter, ahbi shelat, Benjamin Mood, and Kevin Butler. "PCF: A Portable Circuit Format For Scalable Two-Party Secure Computation". *22nd USENIX Security Symposium (Security'13)*, Washington, DC, USA, August 2013.*(Acceptance rate=16.2%.)*
54. Adam Bates, Kevin Butler, Micah Sherr, Clay Shields, Patrick Traynor, and Dan Wallach. "Accountable Wiretapping -or- I Know That You Can Hear Me Now". *19th ISOC Network and Distributed System Security Symposium (NDSS'12)*, San Diego, CA, USA. February 2012. *(Acceptance rate=17.6%)*
55. Kevin Butler, Stephen McLaughlin, and Patrick McDaniel. Rootkit Resistant Disks. *15th ACM Conference on Computer and Communications Security (CCS'08)*, Alexandria, VA, USA. October 2008. *(Acceptance rate=18.1%)*
56. Patrick Traynor, Kevin Butler, William Enck, and Patrick McDaniel. Realizing Massive-Scale Con-

ditional Access Systems Through Attribute-Based Cryptosystems. *15th Annual Network and Distributed System Security Symposium (NDSS'08)*, San Diego, CA, USA. February 2008. *(Acceptance rate=17.8%)*

57. Kevin Butler, William Aiello, and Patrick McDaniel. Optimizing BGP Security by Exploiting Path Stability. *13th ACM Conference on Computer and Communications Security (CCS'06)*, Alexandria, VA, USA, November 2006. *(Acceptance rate=14.8%)*

Other Conference Publications

58. Christian Peeters, Tyler Tucker, Anushri Jain, Kevin Butler, and Patrick Traynor. "LeopardSeal: Detecting Call Interception via Audio Rogue Base Stations". *21st ACM International Conference on Mobile Systems, Applications, and Services (MobiSys'23)*, Helsinki, Finland, June 2023. *Acceptance rate: 20.7%*
59. Washington Garcia, Pin-Yu Chen, Hamilton Scott Clouse, Somesh Jha, and Kevin Butler. "Less is More: Dimension Reduction Finds On-Manifold Adversarial Examples in Hard-Label Attacks". IEEE Conference on Secure and Trustworthy Machine Learning (SatML 2023), Raleigh, NC, USA, February 2023. *Acceptance rate: 25.3%*
60. Daniel Olszewski, Weidong Zhu, Sandeep Sathyanarayana, Kevin Butler, and Patrick Traynor. "HallMonitor: A Framework for Identifying Network Policy Violations in Software". *2022 IEEE Conference on Communications and Network Security (CNS 2022)*, Austin, TX, USA, October 2022. *(Acceptance rate TBD.)*
61. Cassidy Gibson, Vanessa Frost, Katie Platt, Washington Garcia, Luis Vargas, Sara Rampazzi, Vincent Bindschaedler, Patrick Traynor, and Kevin Butler. "Analyzing the Monetization Ecosystem of Stalkerware." *22nd Privacy Enhancing Technologies Symposium (PETS 2022)*, Sydney, Australia, July 2022. *(Acceptance rate: 24%)*
62. Washington Garcia, Scott Clouse, and Kevin Butler. "Disentangling Categorization in Multi-agent Emergent Communication." *2022 Conference of the North American Chapter of the Association for Computational Linguistics (NAACL 2022)*, Seattle, WA, USA, July 2022. *Acceptance rate: 21%*
63. Shantanu Ghosh, Zheng Feng, Kevin Butler, and Mattia Prosperi. "DR-VIDAL: Doubly Robust Variational Information-theoretic Deep Adversarial Learning for Counterfactual Prediction and Treatment Effect Estimation." *2022 American Medical Informatics Association Annual Symposium (AMIA 2022)*, Washington, DC, USA, November 2022.
64. Brendan David-John, Kevin Butler, and Eakta Jain. "For Your Eyes Only: Privacy-Preserving Eye-Tracking Datasets." *14th ACM Symposium on Eye Tracking Research and Applications (ETRA 2022)* Seattle, WA, USA, June 2022. *(Acceptance rate: 42%)*
65. Mounir Elbharabawy, Blas Kojusner, Mohammad Mannan, Kevin Butler, Byron Williams, and Amr Youssef. "SAUSAGE: Security Analysis of Unix domain Socket Usage in Android." *7th IEEE European Symposium on Security and Privacy (Euro S&P'22)*, Genoa, Italy, June 2022. *(Acceptance rate TBD. Best paper finalist.)*
66. Arslan Khan, Joseph Choi, Dave (Jing) Tian, Tyler Ward, Kevin Butler, Patrick Traynor, John M. Shea and Tan Wong. "Privacy-Preserving Localization Using Enclaves." *12th IEEE Ubiquitous Computing, Electronics and Mobile Communication Conference (IEEE UEMCON 2021)*, Virtual Confer-

ence, December 2021.

67. Washington Garcia, Animesh Chhotaray, Joseph Choi, Suman Adari, Kevin Butler, and Somesh Jha. "Brittle Features of Device Authentication." *11th ACM Conference on Data and Application Security and Privacy (CODASPY'21)*, virtual event, April 2021. *(Acceptance rate: 24.5%.)*

68. Joseph Choi, Dave (Jing) Tian, Grant Hernandez, Christopher Patton, Benjamin Mood, Thomas Shrimpton, Patrick Traynor, and Kevin Butler. " A Hybrid Approach to Secure Function Evaluation using SGX." *14th ACM ASIA Conference on Computer and Communications Security (ASIACCS'19)*, Auckland, New Zealand, July 2019. *(Acceptance rate [full papers]: 17%.)*

69. Vanessa Frost, Dave (Jing) Tian, Christie Ruales, Patrick Traynor, and Kevin Butler. "Examining DES-based Cipher Suite Support within the TLS Ecosystem." *14th ACM ASIA Conference on Computer and Communications Security (ASIACCS'19)*, Auckland, New Zealand, July 2019. *(Acceptance rate: 22%.)*

70. Jasmine Bowers, Imani Sherman, Kevin Butler, and Patrick Traynor. "Characterizing Security and Privacy Practices in Emerging Digital Credit Applications." *12th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'19)*, Miami, FL, USA, May 2019. *(Acceptance rate=25.5%)*

71. Dave (Jing) Tian, Joseph Choi, Grant Hernandez, Patrick Traynor, and Kevin Butler. "A Practical Intel SGX Setting for Linux Containers in the Cloud." *9th ACM Conference on Data and Application Security and Privacy (CODASPY'19)*, Dallas, TX, USA, March 2019. *(Acceptance rate=23.5%)*

72. Lianying Zhao, Joseph Choi, Didem Demirag, Kevin Butler, Mohammad Mannan, Erman Ayday, and Jeremy Clark. One-Time Programs Made Practical. *23rd International Conference on Financial Cryptography and Data Security (FC'19)*, St. Kitts, February 2019. *(Acceptance rate=18.5%)*

73. Robert Karam, Tamzidul Hoque, Kevin Butler, and Swarup Bhunia. Mixed-Granular Architectural Diversity for Device Security in the Internet of Things. *Asian Hardware Oriented Security and Trust Symposium (AsianHOST 2017)*, Beijing, China, October 2017.

74. Tyler Ward, Joseph Choi, Kevin Butler, John M. Shea, Patrick Traynor, and Tan Wong. Privacy Preserving Localization Using a Distributed Particle Filtering Protocol. *IEEE MILCOM*, Baltimore, MD, October 2017.

75. Jasmine Bowers, Bradley Reaves, Imani N. Sherman, Patrick Traynor, and Kevin Butler. Regulators, Mount Up! Analysis of Privacy Policies for Mobile Money Services. *13th Symposium on Usable Privacy and Security (SOUPS 2017)*, Santa Clara, CA, July 2017. *(Acceptance rate=26.5%)*

76. Adam Bates, Wajih Ul Hassan, Kevin Butler, Alin Dobra, Brad Reaves, Patrick Cable, Thomas Moyer, and Nabil Schear. Transparent Web Service Auditing via Network Provenance Functions. *26th World Wide Web Conference (WWW 2017)*, Perth, Australia, April 2017. *(Acceptance rate=17.0%)*

77. Benjamin Mood, Debayan Gupta, Henry Carter, Kevin Butler, and Patrick Traynor. "Frigate: A Validated, Extensible, and Efficient Compiler and Interpreter for Secure Computation". *1st IEEE European Symposium on Security and Privacy (Euro S&P 2016)*, Saarbrücken, Germany, March 2016. *(Acceptance rate=17.3%.)*

78. Sriharsha Etigowni, Dave (Jing) Tian, Grant Hernandez, Saman Zonouz, and Kevin Butler. CPAC: Securing Critical Infrastructure with Cyber-Physical Access Control. *32nd Annual Computer Security Applications Conference*, Los Angeles, CA, USA, December 2016. *(Acceptance rate=22.8%)*

79. Thomas Moyer, Patrick Cable, Karishma Chadha, Robert Cunningham, Nabil Schear, Warren Smith, Adam Bates, Kevin Butler, Frank Capobianco, and Trent Jaeger. "Leveraging Data Provenance to Enhance Cyber Resilience". *1st IEEE Cybersecurity Development Conference (SecDev 2016)*, Boston, MA, November 2016. *(Acceptance rate=52.2%.)*

80. Bradley Reaves, Dave Tian, Nolen Scaife, Logan Blue, Patrick Traynor, and Kevin Butler. "Detecting SMS Spam in the Age of Legitimate Bulk Messaging". *9th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'16)*, Darmstadt, Germany, July 2016. *(Acceptance rate=35%.)*

81. Nolen Scaife, Henry Carter, Patrick Traynor, and Kevin Butler. " CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data". *36th IEEE International Conference on Distributed Computing Systems (ICDCS 2016)*, Nara, Japan, June 2016. *(Acceptance rate=17.6%)*

82. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. "Outsourcing Secure Two-Party Computation as a Black Box". *14th International Conference on Cryptology and Network Security (CANS 2015)*, Marrakesh, Morocco, December 2015. *(Acceptance rate=52.9%.)*

83. Dave Tian, Adam Bates, and Kevin Butler. "Defending Against Malicious USB Firmware with GoodUSB". *31st Annual Computer Security Applications Conference (ACSAC 2015)*, Los Angeles, CA, USA, December 2015. *(Acceptance rate=24.4%.)*

84. Ethan Shernan, Henry Carter, Jing (Dave) Tian, Patrick Traynor, and Kevin Butler. "More Guidelines Than Rules: CSRF Vulnerabilities from Noncompliant OAuth 2.0 Implementations". *12th Conference on Detection of Intrustions and Malware and Vulnerability Assessment (DIMVA 2015)*, Milano, Italy, July 2015. *(Acceptance rate=22.7%)*

85. Jing (Dave) Tian, Kevin Butler, Patrick McDaniel, and Padma Krishnaswamy. "Securing ARP From the Ground Up". *5th ACM Conference on Data and Application Security and Privacy (CODASPY 2015)*, San Antonio, TX, USA, March 2015. *(Acceptance rate=33.3%)*

86. Adam Bates, Joe Pletcher, Tyler Nichols, Braden Hollembaek, and Kevin Butler. "Forced Perspectives: Evaluating an SSL Trust Enhancement at Scale". *2014 ACM Internet Measurement Conference (IMC'14)*, Vancouver, BC, Canada, November 2014. *(Acceptance rate=22.9%)*

87. Adam Bates, Benjamin Mood, Masoud Valafar, and Kevin Butler. "Towards Secure Provenance-Based Access Control in Cloud Environments". *3rd ACM Conference on Data and Application Security and Privacy (CODASPY 2013)*, San Antonio, TX, USA, February 2013. *(Acceptance rate=31.8%)*

88. Vasant Tendulkar, Joe Pletcher, Ashwin Shashidharan, Ryan Snyder, Kevin Butler, and William Enck. "Abusing Cloud-based Browsers for Fun and Profit". *28th Annual Computer Security Applications Conference (ACSAC 2012)*, Orlando, FL, USA, December 2012. *(Acceptance rate=19.0%)*

89. Devin J. Pohly, Stephen McLaughlin, Patrick McDaniel, and Kevin Butler. "Hi-Fi: Collecting High-Fidelity Whole-System Provenance". *28th Annual Computer Security Applications Conference (ACSAC 2012)*, Orlando, FL, USA, December 2012. *(Acceptance rate=19.0%)*

90. Benjamin Mood, Lara Letaw, and Kevin Butler. "Memory-Efficient Garbled Circuit Generation for Mobile Devices". *16th IFCA International Conference on Financial Cryptography and Data Security (FC'12)*, Bonaire, February 2012. *(Acceptance rate=26.1%)*

91. Kevin Butler, Stephen McLaughlin, and Patrick McDaniel, "Kells: A Protection Framework for Portable Data". *26th Annual Computer Security Applications Conference (ACSAC 2010)*, Austin, TX,

USA, December 2010. *(Acceptance rate=16.3%)*

92. Machigar Ongtang, Kevin Butler, and Patrick McDaniel. "Porscha: Policy Oriented Secure Content Handling in Android." *26th Annual Computer Security Applications Conference (ACSAC 2010)*, Austin, TX, USA, December 2010. *(Acceptance rate=16.3%)*
93. Kevin Butler, Stephen McLaughlin, and Patrick McDaniel. "Disk-Enabled Authenticated Encryption" (short paper). *26th IEEE Symposium on Massive Storage Systems and Technologies (MSST 2010)*, Incline Village, NV, USA, May 2010. *(Acceptance rate=45.5%.)*
94. Thomas Moyer, Kevin Butler, Joshua Schiffman, Patrick McDaniel, and Trent Jaeger. Scalable Web Content Attestation. *25th Annual Computer Security Applications Conference (ACSAC 2009)*, Honolulu, HI, USA. December 2009. *(Acceptance rate=19.0%.)*
95. William Enck, Kevin Butler, Thomas Richardson, Patrick McDaniel, and Adam Smith. Defending Against Attacks on Main Memory Persistence. *24th Annual Computer Security Applications Conference (ACSAC 2008)*, Anaheim, CA, USA. December 2008. *(Acceptance rate=24.3%)*
96. Dhananjay Bapat, Kevin Butler, and Patrick McDaniel. Towards Automatic Privilege Separation. *3rd International Conference on Information Systems Security (ICISS 2007)*, Delhi, India. December 2007. *(Acceptance rate=25.0%)*
97. Lisa Johansen, Kevin Butler, Michael Rowell, and Patrick McDaniel. Email Communities of Interest. *Fourth Conference on Email and Anti-Spam (CEAS 2007)*, Mountain View, CA, USA. August 2007. *(Acceptance rate=19.0%.)*
98. Anusha Sriraman, Kevin Butler, Patrick McDaniel, and Padma Raghavan. Analysis of the IPv4 Address Space Delegation Structure. *IEEE Symposium on Computers and Communications (ISCC'07)*, Aveiro, Portugal, July 2007. *(Acceptance rate=40%.)*
99. Sunam Ryu, Kevin Butler, Patrick Traynor, and Patrick McDaniel. Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems. *3rd IEEE International Symposium on Security in Networks and Distributed Systems (SSNDS'07)*, Niagara Falls, ON, Canada, May 2007. *(Acceptance rate=40%)*
100. Kevin Butler, Patrick Traynor, William Enck, Jennifer Plasterr, and Patrick McDaniel. Privacy Preserving Web-Based Email. *2nd International Conference on Information Systems Security (ICISS 2006)*, Kolkata, India, December 2006. *(Acceptance rate=30.4%)*
101. Trent Jaeger, Kevin Butler, David King, Serge Hallyn, Joy Latten, and Xiolan Zhang. Leveraging IPsec for Mandatory Per-Packet Access Control. *2nd IEEE Communications Society/CreateNet International Conference on Security and Privacy in Communication Networks (SecureComm'06)*, August 2006. Baltimore, MD, USA. *(Acceptance rate=25.4%.)*
102. Kevin Butler and Patrick McDaniel, Understanding Mutable Internet Pathogens, or How I Learned to Stop Worrying and Love Parasitic Behavior. *1st International Conference on Information Systems Security (ICISS 2005)*, December 2005. Kolkata, India. *(Invited paper.)*

Workshop Publications

103. Jennifer Sheldon, Weidong Zhu, Adnan Abdulla, Kevin Butler, Md Jahidul Islam, and Sara Rampazzi. "Position: Deep Note: Can Acoustic Interence Damage the Availability of Hard Disk Storage

in Underwater Data Centers?" *15th ACM Workshop on Hot Topics in Storage and Files Systems (HotStorage 2023)*, Boston, MA, USA, July 2023. *Best Paper Award.*

104. Brendan David-John, Diane Hosfelt, Kevin Butler, and Eakta Jain. "Let's SOUP Up XR: Collected thoughts from an IEEE VR workshop on privacy in mixed reality." *1st International Workshop on Security for XR and XR for Security (VR4Sec), in conjunction with SOUPS 2021*, virtual event, August 2021.

105. Sushrut Shringarputale, Patrick McDaniel, Kevin Butler, and Thomas La Porta. "Co-residency Attacks on Containers are Real." *2020 ACM Cloud Computing Security Workshop (CCSW'20)*, Orlando, FL, USA, November 2020.

106. Suman Adari, Washington Garcia, and Kevin Butler. "Adversarial Video Captioning". *2019 Dependable and Secure Machine Learning Workshop (DSML'19)*, Portland, OR, USA, June 2019.

107. Siddhant Deshmukh, Henry Carter, Grant Hernandez, Patrick Traynor, and Kevin Butler. "Efficient and Secure Template Blinding for Biometric Authentication". *2nd IEEE Workshop on Security and Privacy in the Cloud (SPC 2016)*, Philadelphia, PA, USA, October 2016.

108. Debayan Gupta, Benjamin Mood, Joan Feigenbaum, Kevin Butler and Patrick Traynor. "Using Intel Software Guard Extensions for Efficient Two-Party Secure Function Evaluation." *2016 Workshop on Encrypted Computing and Applied Homomorphic Cryptography (WAHC'16)*, Barbados, February 2016.

109. Adam Bates, Kevin Butler, and Thomas Moyer. "Take Only What You Need: Leveraging Mandatory Access Control Policy to Reduce Provenance Storage Costs." *7th Annual Workshop on Theory and Practice of Provenance (TaPP'15)*, Edinburgh, Scotland, July 2015.

110. Adam Bates, Kevin Butler, Andreas Haeberlen, Micah Sherr, and Wenchao Zhou. "Let SDN Be Your Eyes: Secure Forensics in Data Center Networks." *NDSS Workshop on Security of Emerging Network Technologies (SENT)*, San Diego, CA, USA, February 2014.

111. Matt Bishop, Emily Rine Butler, Kevin Butler, Carrie Gates, and Steven Greenspan. "Forgive and Forget: Return to Obscurity". *New Security Paradigms Workshop (NSPW 2013)*, Banff, AB, Canada, September 2013.

112. Peter McKay, Bryan Clement, Sean Haverty, Elijah Newton, and Kevin Butler. "Read My Lips: Towards Use of the Microsoft Kinect as a Visual-Only Automatic Speech Recognizer." *2013 Workshop on Home Usable Privacy and Security (HUPS)*, Newcastle, UK, July 2013.

113. Adam Bates, Benjamin Mood, Joe Pletcher, Hannah Pruse, Masoud Valafar, and Kevin Butler. "Detecting Co-Residency with Active Traffic Analysis Techniques". *4th ACM Cloud Computing Security Workshop (CCSW 2012)*, Raleigh, NC, USA, October 2012. *(Acceptance rate=12.0% for full papers.)*

114. Lara Letaw, Joe Pletcher, and Kevin Butler. "Host Identification via USB Fingerprinting". *6th IEEE International Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE 2011)*, Oakland, CA, USA, May 2011. *(Acceptance rate=34.8%.)*

115. Kevin Butler, William Enck, Harri Hursti, Stephen McLaughlin, Patrick Traynor, and Patrick McDaniel. Systemic Issues in the Hart InterCivic and Premier Voting Systems: Reflections Following Project EVEREST. *2008 USENIX/ACCURATE Electronic Voting Workshop (EVT'08)*, July 2008. San Jose, CA, USA. *(Acceptance rate=44.1%)*

116. Shiva Chaitanya, Kevin Butler, Anand Sivasubramaniam, Patrick McDaniel and Murali Vilayan-

nur. Design, implementation and evaluation of security in iSCSI-based network storage systems. *2nd International Workshop on Storage Security and Survivability (StorageSS 2006)*, October 2006. Alexandria, VA, USA. *(Acceptance rate=68%)*

117. Patrick McDaniel, Kevin Butler, Stephen McLaughlin, Radu Sion, Erez Zadok, and Marianne Winslett. "Towards a Secure and Efficient System for End-to-End Provenance". *USENIX Workshop on Theory and Practice of Provenance (TaPP)*, February 2010. *(Acceptance rate=68.8%)*

118. Kevin Butler and Petros Efstathopoulos. U Can't Touch This: Block-Level Protection for Portable Storage. *International Workshop on Software Support for Portable Storage (IWSSPS 2009)*, October 2009. Grenoble, France.

119. Kevin Butler, Stephen McLaughlin, and Patrick McDaniel. Non-Volatile Memory and Disks: Avenues for Policy Architectures. *1st Computer Security Architectures Workshop (CSAW 2007)*, November 2007. Fairfax, VA, USA. *(Acceptance rate=30%)*

120. Kevin Butler and Patrick McDaniel, Testing Large Scale BGP Security in Replayable Network Environments. *DETER Community Workshop on Cyber Security Experimentation and Test*, June 2006. Arlington, VA, USA.

121. Sophie Qiu, Kevin Butler, and Patrick McDaniel, BGPRV: Retrieving and Processing BGP Data with Efficiency and Convenience. *DETER Community Workshop on Cyber Security Experimentation and Test*, June 2006. Arlington, VA, USA.

Technical Reports

122. Efe Bozkir, Süleyman Özdel, Mengdi Wang, Brendan David-John, Hong Gao, Kevin Butler, Eakta Jain, and Enkelejda Kasneci. "Eye-tracked Virtual Reality: A Comprehensive Survey on Methods and Privacy Challenges." *arXiv:2305.14080*, May 2023.

123. Washington Garcia, Pin-Yu Chen, Somesh Jha, Scott Clouse, and Kevin Butler. "Hard-label Manifolds: Unexpected Advantages of Query Efficiency for Finding On-manifold Adversarial Examples." *arXiv:2013.03325*, March 2021.

124. Kevin Butler. "Digital Financial Services security audit guideline." Security, Infrastructure and Trust Working Group, Financial Inclusion Global Initiative, published by International Telecommunications Union (ITU), March 2021.

125. Kevin Butler and Vijay Mauree. "Digital Financial Services security assurance framework." Security, Infrastructure and Trust Working Group, Financial Inclusion Global Initiative, published by International Telecommunications Union (ITU), January 2021.

126. Washington Garcia, Joseph Choi, Suman Adari, Somesh Jha, and Kevin Butler. "Explainable Black-Box Attacks Against Model-based Authentication." *arXiv:1810.00024*, September 2018.

127. Kevin Butler, Patrick Traynor, and Tiago Novais. "MM App Security Best Practices." Official Document MM.01, GSM Association, London, United Kingdom, June 2018.

128. Kevin Butler, Leon Perlman, Paul Makin, Henry Gerwitz, Patrick Traynor, Yury Grin, Evgeniy Bondarenko, and Richard Miller. "ITU-T Focus Group Digital Financial Services: Security Aspects of Digital Financial Services (DFS)." Focus Group Technical Report, International Telecommunications Union, Geneva, Switzerland, January 2017.

129. Adam Bates, Joe Pletcher, Tyler Nichols, Braden Hollembaek, and Kevin Butler. "Towards Usable System-Wide Trust Agility." Technical Report CIS-TR-2013-13, Department of Computer and Information Science, University of Oregon, Eugene, OR, October 2013.

130. Benjamin Mood and Kevin Butler. "Optimizing Secure Function Evaluation for Mobile Devices". Technical Report CIS-TR-2013-10, Department of Computer and Information Science, University of Oregon, Eugene, OR, September 2013.

131. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. "Secure Outsourced Garbled Circuit Evaluation for Mobile Devices". Technical Report GT-CS-12-09, College of Computing, Georgia Institute of Technology, Atlanta, GA, December 2012.

132. Kevin Butler and Petros Efstathopoulos. U Can't Touch This: Block-Level Protection for Portable Storage. Technical Report Symantec-SRL/MV2009-11, Symantec Research Labs, Mountain View, CA, June 2009.

133. Kevin Butler, Stephen McLaughlin, Thomas Moyer, Joshua Schiffman, Patrick McDaniel, and Trent Jaeger. Firma: Disk-Based Foundations for Trusted Operating Systems. Technical Report NAS-TR-0114-2009, Networking and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, May 2009.

134. Kevin Butler, Stephen McLaughlin, Thomas Moyer, Patrick McDaniel, and Trent Jaeger. SwitchBlade: Policy-Driven Disk Segmentation. Technical Report NAS-TR-0098-2008, Networking and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, November 2008.

135. P. McDaniel, K. Butler, W. Enck, H. Hursti, S. McLaughlin, P. Traynor, M. Blaze, A. Aviv, P. Cerny, S. Clark, E. Cronin, G. Shah, M. Sherr, G. Vigna, R. Kemmerer, D. Balzarotti, G. Banks, M. Cova, V. Felmetsger, W. Robertson, F. Valeur, J. Hall, and L. Quilter, EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing. Public Report, Ohio Secretary of State, December 2007.

136. Kevin Butler, Stephen McLaughlin, Patrick McDaniel, and Youngjae Kim. Autonomously Secure Disks. Technical Report NAS-TR-0072-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, May 2007. (*Updated September 2007.*)

137. Lisa Johansen, Kevin Butler, William Enck, Patrick Traynor, and Patrick McDaniel. Grains of SANs: Building Storage Area Networks from Memory Spots.Technical Report NAS-TR-0060-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, January 2007.

138. Luke St. Clair, Lisa Johansen, Kevin Butler, William Enck, Matthew Pirretti, Patrick Traynor, Patrick McDainel, and Trent Jaeger. Password Exhaustion: Predicting the End of Password Usefulness. Technical Report NAS-TR-0030-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, May 2006. (*Updated January 2007.*)

Articles for Media

139. Patrick Traynor and Kevin Butler. "Mobile money in developing countries: study reveals secu-

rity flaws in apps". *The Guardian.* 24 September 2015. `http://www.theguardian.com/global-development-professionals-network/2015/sep/24/mobile-money-apps-security-flaws-study-reveals?CMP=twt_gu`

Patents

U.S. Patent 8,856,918, Host validation mechanism for preserving integrity of portable storage data. Petros Efstathopulos, Bruce Montague, Dharmesh Shah, Kevin Butler. October 7, 2014.
U.S. Patent 10,685,114, Malware Detection Via Data Transformation Monitoring. Walter N. Scaife, Kevin Butler, Henry Carter, Patrick G. Traynor. June 16, 2020.
U.S. Patent 11,265,717, Detecting SS7 Redirection Attacks with Audio-Based Distance Bounding. Patrick G. Traynor, Christian Peeters, Bradley G. Reeves, Hadi Abdullah, Kevin Butler, Jasmine Bowsers, Walter N. Scaife. March 1, 2022.
U.S. Patent 11,568,044, Method and Apparatus For Vetting Universal Serial Bus Device Firmware. Kevin Butler, Tuba Yavuz, Jing Tian, Grant Hernandez, Farhaan Fowze. January 31, 2023.
U.S. Patent 11,640,464, Protocol Model Learning and Guided Firmware Analysis. Tuba Yavuz, Farhaan Fowze, Kevin Raymond Boyce Butler, Jing Tian, Grant Haydock Hernandez. May 2, 2023.
U.S, Patent 11,663,388, Automated Security Analysis of Baseband Firmware. Grant Haycock Hernandez, Kevin R. Butler, Patrick G. Traynor. May 31, 2023.

Teaching

University of Florida

- *CIS 4360: Computer and Information Security*, undergraduate, Fall 2020, Fall 2019, Fall 2018, Fall 2017.
- *CIS 5370: Computer and Information Security*, graduate, Spring 2023, Spring 2019, Spring 2018, Spring 2017.
- *CIS 6930: Special Topics: Mobile and Embedded System Security*, graduate, Spring 2020.
- *CNT 5410: Computer and Network Security*, graduate, Fall 2015.

University of Oregon

- *CIS 415: Operating Systems (substantially revised)*, Spring 2014, Spring 2013, Spring 2012, Spring 2011.
- *CIS 607: Seminar on Generating Trustworthy Data (new)*, Winter 2014.
- *CIS 607: Seminar on Embedded Systems and Security (new)*, Spring 2013.
- *CIS 433/533: Computer and Network Security*, Winter 2013, Winter 2011.
- *CIS 607: Seminar on Computer Security in the Physical World (new)*, Spring 2012.
- *CIS 330: C/C++ and UNIX (substantially revised)*, Winter 2012.
- *CIS 610: Advanced Topics in Systems Security (new)*, Fall 2011.
- *CIS 607: Seminar on Security in Systems, Storage, and Clouds (new)*, Fall 2010.

The Pennsylvania State University

- *EE/CSE 458: Computer Networks*, Summer 2006.

Professional Service

Editorial Positions, Panels, and Boards

Editorial Boards:

Associate Editor, ACM Transactions on Security and Privacy (TOPS), 2021-present.

Associate Editor, Journal of Computer Security, 2020-present.

Associate Editor, IEEE Transactions on Dependable and Secure Computing *(Impact Factor: 4.41)*, 2019-2023.

Associate Editor, ACM Digital Threats: Research and Practice, 2017-2022.

Editorial Board, International Journal of Cybersecurity Science and Technology, 2017-2022.

Review Board, IEEE Systems Journal, Special Issues on Security and Privacy in Complex Systems, 2012.

Scientific Grant Panels:

Review Panelist, National Science Foundation, 2022, 2021, 2020, 2018, 2017, 2016, 2014 (2), 2013, 2012.

Review Panelist, American Association for the Advancement of Science (AAAS), 2019.

Grant Reviewer, Austrian Science Fund, 2018.

Grant Reviewer, Natural Science and Engineering Research Council of Canada, 2022, 2019, 2018, 2017.

Grant Reviewer, Israel Science Foundation, 2016.

Conference Steering Committees:

Steering Committee Member, ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2019 *-present.*

Steering Committee Member, Annual Computer Security Applications Conference, 2014 *-present.*

Service to National and International Organizations:

Council Member, Computing Research Association Computing Community Consoritum, 2023-present.

Co-Chair, Security, Infrastructure, and Trust Working Group, Financial Inclusion Global Initiative, International Telecommunications Union, 2017-2022.

Co-Chair and Leader of Security Workstream, Technology, Innovation, and Competition Working Group, Focus Group on Digital Financial Services, International Telecommunications Union, 2015-2016.

Conference & Workshop Chairships

1. **Technical Program Co-Chair**, 32nd USENIX Security Symposium (USENIX Security'22), Boston, MA, USA, August 2022.
2. **Conference General Chair**, 36th and 37th Annual Computer Security Applications Conference (ACSAC'20, ACSAC'21), Austin, TX, USA, 2020,2021.
3. **Technical Program Co-Chair**, 16th EAI International Conference on Security and Privacy in Communication Networks (Securecomm 2020), Washington, DC, USA, October 2020.
4. **Technical Program Co-Chair**, 2020 USENIX Summit on Hot Topics in Security (HotSec'20), Boston, MA, USA, August 2020 *(suspended due to COVID-19 pandemic)*
5. **Technical Program Co-Chair**, 11th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'18), Stockholm, Sweden, July 2018.
6. **Conference General Chair**, 38th IEEE Symposium on Security and Privacy, San Jose, CA, May 2017.
7. **Vice Chair and Registration Chair**, 37th IEEE Symposium on Security and Privacy, San Jose, CA, May 2016.
8. **Technical Program Chair**, 30th Annual Computer Security Applications Conference (ACSAC 2014), New Orleans, LA, December 2014.
9. **Technical Program Co-Chair**, 29th Annual Computer Security Applications Conference (ACSAC 2013), New Orleans, LA, December 2013.

Other Conference & Workshop Organization Activities (118 Tech. Program Committees)

Top-4 Security Conferences

10. **USENIX Security Symposium**: *TPC Member*, 2021, 2020, 2019, 2018, 2017, 2015, 2014; *Short Talks Co-Chair*, 2017.
11. **IEEE Symposium on Security and Privacy (Oakland)**: *TPC Member*, 2024, 2023, 2021, 2020, 2018, 2017, 2016, 2012; *Publications Chair*, 2014, 2013, 2012, 2011, *Submissions Chair*, 2008.
12. **ISOC Network and Distributed Security Symposium (NDSS)**: *TPC Member*, 2021, 2020, 2019, 2018, 2017, 2016.
13. **ACM Conference on Computer and Communications Security (CCS)**: *TPC Member*, 2020, 2016, 2015, 2014, 2013; *TPC Member (Industry Track)*, 2007, 2004.

Other Conferences and Workshops

14. **Privacy Enhancing Technologies Symposium (PETS)/Journal of Privacy Enhancing Technologies**, *Senior PC Member*, 2023, *TPC Member/Editorial Board*, 2014-2016.
15. **IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)**: *TPC Member*, 2023.
16. **ACM Conference on Security in Wireless and Mobile Networks (WiSec)**: *TPC Member*, 2023, 2022, 2021, 2020, 2019, 2017, 2016, 2015, 2014.
17. **IEEE Secure Development Conference (SecDev)**: *TPC Member*, 2023, 2022.
18. **USENIX Annual Technical Conference (ATC)**: *TPC Member*, 2021, 2020.
19. **IEEE European Symposium on Security and Privacy (Euro S&P)**: *TPC Member*, 2020.
20. **USENIX Workshop on Cyber Security Experimentation and Test (CSET)**: *TPC Member*, 2019, 2015, 2014, 2013.
21. **International Workshop on the Theory and Practice of Provenance (TaPP)**: *TPC Member*, 2019.
22. **USENIX Enigma Conference**: *TPC Member*, 2019, 2018.
23. **ACM Cloud Computing Security Workshop (CCSW)**: *TPC Member*, 2019, 2014.
24. **International Provenance and Annotation Workshop (IPAW)**: *TPC Member*, 2018
25. **ACM Symposium on Information, Computer and Communications Security (ASIACCS)**: *TPC Member*, 2018, 2017, 2015, 2014.
26. **Annual Computer Security Applications Conference (ACSAC)**: *TPC Member*, 2018, 2017, 2012, 2011; *Test of Time Awards Chair*, 2019; *Panels Chair*, 2012, 2011; *Publicity Chair*, 2010.
27. **World Conference on Informaton Security Applications (WISA)**: *TPC Member*, 2017.
28. **International Conference on Cryptology and Network Security (CANS)**: *TPC Member*, 2017.
29. **New Security Paradigms Workshop (NSPW)**: *TPC Member*, 2016, 2015, 2014, 2013.
30. **IEEE Mobile Security Technologies Workshop (MOST)**: *TPC Member*, 2015, 2014.
31. **Symposium and Bootcamp on the Science of Security (HotSoS)**: *TPC Member*, 2015.
32. **Workshop on Encrypted Computing and Applied Homomorphic Cryptography (WAHC)**: *TPC Member*, 2015.
33. **European Symposium on Research in Computer Security (ESORICS)**: *TPC Member*, 2014, 2013, 2012.
34. **Smart Energy Grid Security Workshop (SEGS)**: *TPC Member*, 2014, 2013.
35. **Conference on Privacy, Security and Trust (PST)**: *TPC Member*, 2014, 2013.
36. **Global Internet Symposium (GI)**: *TPC Member*, 2014.
37. **IEEE International Conference on Big Data (BigData)**: *TPC Member*, 2013.
38. **IEEE LCN Network Security Workshop (WNS)**: *TPC Member*, 2013.
39. **International Workshop on Security in Information Systems (WOSIS)**: *TPC Member*, 2013,

2012.

40. **International Conference on Applied Cryptography and Network Security (ACNS)**: *TPC Member*, 2013.
41. **International Workshop on Security (IWSEC)**:, *TPC Member*, 2012, 2008, 2007.
42. **Workshop on Secure Network Protocols (NPSec)**: *Publicity Chair*, 2012.
43. **LCN Workshop on Security in Communication Networks (SICK)**: *TPC Member*, 2012.
44. **USENIX Workshop on Hot Topics in Security (HotSec)**: *TPC Member*, 2012.
45. **International Workshop on Security (IWSEC)**: *TPC Member*, 2011, 2010.
46. **International Conference on Security and Privacy in Communication Networks (SecureComm)**: *TPC Member*, 2011.
47. **International Conference on Availability, Reliability and Security (ARES)**: *TPC Member*, 2011, 2010, 2009, 2008, 2007.
48. **International Conference on Internet Monitoring and Protection (ICIMP)**: *TPC Member*, 2011, 2010.
49. **International Conference on Financial Cryptography and Data Security (FC)**: *TPC Member*, 2011.
50. **International Conference on Information Systems Security (ICISS)**: *TPC Member*, 2009, 2008, 2007; *Submissions and Web Chair*, 2007.
51. **IEEE International Workshop on Software Security Process**: *TPC Member*, 2009.
52. **International Conference on International Conference on Information Security and Assurance (ISA)**: *TPC Member*, 2009, 2008; *Publicity Co-Chair*, 2008.
53. **International Workshop on Security in Systems and Networks (SSN)**: *TPC Member*, 2009, 2007.
54. **Conference on Future Generation Communication and Networking (FGCN)**: *TPC Member*, 2008, 2007.
55. **IEEE International Workshop on Security in Software Engineering (IWSSE)**: *TPC Member*, 2008, 2007.
56. **IEEE/IFIP Conference on Dependable Systems and Networks (DSN)**: *TPC Member (Fast Abstracts)*, 2008.
57. **International Workshop on Secure Software Engineering (SecSE)**: *TPC Member*, 2008.

Conference Session Chair: USENIX Security'18, ACSAC'17, WWW'17, IEEE SP'16, CCS'16, CCS'14, HotSec'12, IEEE SP'12, CCS'09

Journal & Book Reviewing

IEEE Transactions on Dependable and Secure Computing (TDSC), 2019, 2014, 2010; Communications of the ACM (CACM), 2019; IEEE Transactions on Computers (TC), 2019, 2012, 2009; IEEE Security and Privacy, 2018, 2013, 2010; Journal of Computer Security (JCS), 2018; IEEE Transactions on Information Forensics and Security (TIFS), 2017, 2013, 2011; Journal of Internet Services and

Applications (JISA), 2017; ACM Transactions on Information and System Security (TISSEC), 2016, 2015, 2014, 2010, 2009, 2008, 2006; IEEE Transactions on Reliability (TR), 2014; ACM Transactions on Internet Technologies (TOIT), 2013, 2010, 2009; ACM Computing Surveys, 2013; ACM Transactions on Storage (TOS), 2013, 2011; Elsevier Computers and Security, 2013, 2011; International Journal of Computer Mathematics, 2011; IEEE Transactions on Parallel and Distributed Systems (TPDS), 2011, 2008; Wiley and Sons (Book proposal reviewer), 2010; EURASIP Journal on Information Security (JIS), 2011, 2010; Elsevier Journal of Computer Networks, 2010, 2005; International Journal of Software and Informatics (IJSI), 2010; International Journal of Security and Networks (IJSN), 2009, 2007; The Computer Journal (Oxford), 2009; ACM/IEEE Transactions on Networking (TON), 2008; Wireless Personal Communications, 2008; IEEE Communications Surveys and Tutorials, 2007; IEEE Transactions on Software Engineering (TSE), 2007; Software: Practice and Experience, 2007; Handbook of Information Security, 2004.

Conference & Workshop Reviewing

USENIX OSDI, 2016; IEEE INFOCOM, 2014, 2007; IEEE Symposium on Security and Privacy (S&P), 2013, 2009, 2008, 2007; ISOC Symposium on Network and Distributed Systems Security (NDSS), 2013, 2012, 2009, 2007; ACM Conference on Data and Application Security and Privacy (CODASPY), 2013; IEEE Computer Security Foundations Symposium (CSF), 2011; ACM Symposium on Computer and Communications Security (CCS), 2010, 2009, 2008, 2006; Annual Computer Security Applications Conference (ACSAC), 2010, 2007, 2006, 2005; USENIX Workshop on Hot Topics in Security (HotSec), 2010, 2007; ACM Symposium on Access Control Models and Technologies (SACMAT), 2010, 2009, 2008, 2006; IFCA International Conference on Financial Cryptography and Data Security (FC), 2010, 2008, 2007; Information Security Conference (ISC), 2009; USENIX Security Symposium, 2009, 2008, 2007, 2006, 2004; IEEE GLOBECOM, 2008; IFIP Conference on Data and Applications Security (DBSEC), 2008, 2006; USENIX Conference on File and Storage Technologies (FAST), 2008; IEEE International Conference on Computer Engineering and Systems (ICCES), 2007; IEEE International Conference on Distributed Computing Systems (ICDCS), 2007; IEEE Sarnoff Symposium, 2007; IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2007; ACM International Workshop on Storage Security and Survivability (StorageSS), 2006; International Workshop on Security (IWSEC), 2006; International Conference on Emerging Trends in Computer Science (ETRICS), 2006; International Conference on Applied Cryptography and Network Security (ACNS), 2006; European Symposium on Research in Computer Security (ESORICS), 2005.

University Service

Sabbatical Committee, Member, College of Engineering, University of Florida, 2021-present.

Steering Committee, Member, University of Florida, 2018-present.

Graduate Admissions Committee, Member, CISE, University of Florida, 2019-present.

Consortium for Media and Trust Director Search Committee, Member, University of Florida, 2019.

Faculty Search Committee, Chair, CISE, University of Florida, 2018-2021.

Faculty Search Committee, Member, CISE, University of Florida, 2017-2018.

Awards Committee, Member, CISE, University of Florida, 2015-present.

Graduate Affairs Committee, Member, CISE, University of Florida, 2014-2018.

Graduate Education Committee, Member, CIS, University of Oregon, 2010-2014.

Undergraduate Curriculum Committee, Member, CIS, University of Oregon, 2012-2014.

General Education Committee, Member, University of Oregon, 2013-2014.

Students

Graduate Advisees

Past Ph.D Advisees:

- Washington Garcia, Fall 2022, now **Research Scientist**, University of Dayton Research Institute.
- Grant Hernandez, Summer 2020, now **Senior Security Engineer**, Qualcomm.
- Dave (Jing) Tian, Summer 2019, now **Assistant Professor of Computer Science**, Purdue University (NSF CAREER award, 2022).
- Adam Bates, Summer 2016, now **Associate Professor of Computer Science**, University of Illinois at Urbana-Champaign (NSF CAREER award, 2018).
- Benjamin Mood Spring 2016, now **Assistant Professor of Computer Science**, Point Loma Nazarene University.

Current Ph.D. Advisees: Yunhao Wu (PhD, Spring 2024), Weidong Zhu (PhD, Spring 2024, co-advised with Sara Rampazzi), Cassidy Gibson (PhD, Spring 2025, co-advised with Patrick Traynor), Anna Crowder (PhD, Spring 2026), Caroline Fedele (PhD, Spring 2026), Magdalena Pasternak (PhD, Spring 2026), Carson Stillman (PhD, Spring 2028), Kevin Childs (PhD, Spring 2030).
Past Master's Degree Students: Benjamin Simon (MS, Spring 2023), Reza Shahriari (MS, Fall 2023), Blas Kojusner (MS, Fall 2022), Hunter Searle (MS, Summer 2022), Vanessa Frost (MS, Spring 2022), Joseph Choi (MS, Spring 2021), Joseph Pletcher (MS, Spring 2013), Adam Bates (MS, Spring 2012), Benjamin Mood (MS, Spring 2012), Masoud Valafar (MS, Fall 2011).

Other Graduate Student Advising

PhD Committee Member: Ghulam Memon (PhD, University of Oregon, Fall 2013), Saeed Sadeghian (PhD, University of Calgary, Fall 2015), Henry Carter (PhD, Georgia Institute of Technology, Spring 2016), Mehdi Sadi (PhD, University of Florida, Spring 2017), Bradley Reaves (PhD, University of

Florida, Summer 2017), Robert Karam (PhD, University of Florida, Summer 2017), Luka Malisa (PhD, ETH Zurich, Summer 2017), Fengchao Zhang (PhD, University of Florida, Spring 2018), Kai Yang (PhD, University of Florida, Summer 2018), Nolen Scaife (PhD, University of Florida, Spring 2019), Ruimin Sun (PhD, University of Florida, Spring 2019), Francesco Pittaluga (PhD, University of Florida, Spring 2019), Jonathan Smith (PhD, University of Florida, Spring 2020), Beong Heyn Kim (PhD, University of Toronto, Spring 2020), Christopher Patton (PhD, University of Florida, Summer 2020), Xiaoyong Yuan (PhD, University of Florida, Summer 2020), Farhaan Fowze (PhD, University of Florida, Summer 2020), Tamzidul Hoque (PhD, University of Florida, Summer 2020), Jasmine Bowers (PhD, University of Florida, Summer 2020), Olufemi Odegbile (PhD, University of Florida, Spring 2021), Luis Vargas (PhD, University of Florida, Spring 2021), Atul Prasad Deb Nath (PhD, University of Florida, Spring 2021), Abdulrahman Alaqi (PhD, University of Florida, Spring 2021), Aritra Dhar (PhD, ETH Zurich, Summer 2021), Olufemi Odegbile (PhD, University of Florida, Summer 2021), Yazhou Tu (PhD, University of Louisiana at Lafayette, Fall 2021), Shubhra Deb Paul (PhD, University of Florida, Spring 2022), Hadi Abdullah (PhD, University of Florida, Spring 2022), Christian Peeters (PhD, University of Florida, Summer 2022), Brendan David-John (University of Florida, Summer 2022), Sarah Amir (PhD, University of Florida, Summer 2022), Jonathan Cruz (PhD, University of Florida, Fall 2022), Logan Blue (PhD, University of Florida, Spring 2023), Animesh Chhotaray (PhD, University of Florida, Spring 2023), Martin Georgiev (PhD, University of Oxford, Spring 2023), Sujan Kumar Saha (PhD, University of Florida, Spring 2023), Minh Vu (PhD, University of Florida, Spring 2024), Chaoyi Ma (PhD, University of Florida, Spring 2023), Yihang (Ken) Bai (PhD, University of Florida, Spring 2024), Anurag Swarnim Yadav (PhD, University of Florida, Spring 2024), Manish Merugu (PhD, University of Florida, Spring 2025), Yichen Jian (PhD, University of Florida, Spring 2025), Christopher Brant (PhD, University of Florida, Spring 2025), Mohammad Sami Ul Islam Sami (PhD, University of Florida, Spring 2025), Seth Layton (PhD, University of Florida, Spring 2026). Ethan Wilson (PhD, University of Florida, Spring 2026), Wenxuan Bao (PhD, Univesrity of Florida, Spring 2026).
Other Committee Membership: Ming Liu (University of Florida, thesis proposal committee, Spring 2016), Reza Motamedi (University of Oregon, thesis proposal committee, Spring 2014), Jason Gustafson (Univeristy of Oregon, MS Committee, Winter 2012), Amir Amir Farzad (University of Oregon, MS committee, Spring 2013).

Undergraduate Students

Hannah Pruse (Honors BS, Oregon, Spring 2013 - **NSF Graduate Fellow**), Ryan Leonard (Honors BS, Oregon, Spring 2013), Peter McKay (Honors BS, Oregon, Spring 2013), Braden Hollembaek (Honors BS, Oregon, Spring 2014), Abdul Alkhelaifi (Honors BS, Oregon Spring 2014), Devan Patel (BS, Florida, Spring 2015), Cynthia Omauzo (CS, Prarie View A&M, CRA DREU, hosted Summer 2015), Jared Trinkler (BS, University Scholar, Florida, Spring 2017), Joshua Uduehi (CRA DREU, BS, Indiana University, hosted Summer 2017), Suman Adari (BS, Florida, Spring 2021), Christie Ruales (BS, CRA/ACSA SWSIS Scholar, University Scholar, Florida, Spring 2021), César Arguello (BS, Florida, Spring 2022), Katie Platt (BS, Florida, Fall 2022), Gabriella Neris (BS, Florida, Spring 2023).

Presentations & Invited Talks

1. **Keynote Address:** From Blue Boxes to Black Boxes: Adventures in Uncovering Device Function-

ality. *IEEE Workshop on Offensive Technology (WOOT)*, San Francisco, CA, May 2013.

2. From Blue Boxes to Black Boxes: Telecommunications Security Research at the Florida Institute for Cybersecurity Reserach.. *Florida Cybersecurity Advisory Council*, Gainesville, FL, May 2013.
3. Privacy-Preserving Computation for Resource-Constrained Devices. *NATO Science and Technology Office ET Meeting*, Washington, DC, November 2022.
4. Invstigating External Surfaces in Android Devices. *Microsoft Research*, Cambridge, United Kingdom, February 2020.
5. Firmware-Informed Approaches to Securing Systems and Devices. *ARM Research*, Cambridge, United Kingdom, February 2020.
6. Cybersecurty and Election Security: Innovations in Research and Technology (with Juan Gilbert). *Orange and Blue Plate Luncheon*, Tallahassee, FL, February 2020.
7. Making MPC More Accessible Through Informed Compiler Design. *Workshop on Teaching Secure Computation*, Washington, DC, January 2020.
8. Analyzing Applications to Assess Security. *FIGI Security Clinic*, Geneva, Switzerland, December 2019.
9. Application Security Framework for DFS. *FIGI Security Clinic*, Geneva, Switzerland, December 2019.
10. Security Research at the Florida Insitute for Cybersecurity Research (with Patrick Traynor). *UF Eye Opener Breakfast*, Gainesville, FL, USA, October 2019.
11. "Plug and Pray" Today: Reflecting on a Decade of Peripheral Security Research. *UCLA*, Los Angeles, CA, USA, April 2019.
12. Cybersecurity Challenges in a Diverging Internet. *Jean Monnet Centre of Excellence Annual Workshop on the European Union*, Gainesville, FL, USA, April 2019.
13. Designing a Security Management Framework for Digital Financial Services. *ITU Security, Infrastructure, Trust Working Group Meeting*, Washington, DC, USA, April 2019.
14. Developing a Consortium on Trust in Media and Technology. *Invited Panelist. University of Florida Foundation National Board Meeting*, Atlanta, GA, USA, March 2019.
15. Designing a Security Management Framework for Digital Financial Services. *Financial Inclusion Global Symposium*, Cairo, Egypt, January 2019.
16. Staying Safe in Cyberspace: Understanding the Threats and Defenses. *The Village at Gainesville*, Gainesville, FL, USA, October 2018.
17. Domain Informed Techniques for IoT Security (with Tuba Yavuz). *ARM Research*, San Jose, CA, USA, October 2018.
18. A Discussion on Security Education in Academia. *Invited Panelist. ACM Conference on Communications and Communication Security (CCS)*, Toronto, ON, Canada, October 2018.
19. New Attack Surfaces Against Mobile Platforms. *Columbia University Cybersecurity and Payments Roundtable*, New York, NY, August 2018.
20. **Keynote Address:** Secure and Efficient Whole-System Data Provenance: A Retrospective. *2nd Workshop on Provenance-based Security*, London, UK, July 2018.
21. "Plug and Pray" Today: Reflecting on a Decade of USB Security Research. *University of Oxford*,

Oxford, UK, July 2018.

22. "Plug and Pray" Today: Reflecting on a Decade of USB Security Research. *Chinese Academy of Sciences*, Beijing, China, June 2018.
23. Characterizing Tooling and Interfaces for Mobile Applications and Devices. *Samsung Research America*, Mountain View, CA, USA, May 2018.
24. "Plug and Pray" Today: Reflecting on 10 Years of USB Security Research. *Symantec Research Labs*, Culver City, CA, USA, May 2018.
25. A Security Framework for for DFS Featurephone Applications. *ITU FIGI Security, Information, and Trust Working Group Meeting*, Washington, DC, USA, April 2018.
26. Application Security for DFS Featurephone Applications. *Financial Inclusion Global Initiative Symposium*, Bangalore, India, November 2017.
27. Towards More Robust Interactions with Telephones and Peripherals (with Patrick Traynor). *Florida International University*, Miami, FL, October 2017.
28. **Keynote Address:** Making USB Safer for Hosts and Peripherals. *Third International Conference on Future Network Systems and Security (FNSS 2017)*, Gainesville, FL, August 2017.
29. Making USB Safer for Hosts and Peripherals. *ETH Zurich*, Zurich, Switzerland, July 2017.
30. Security Challenges in Mobile Devices. *FinTech, DFS and Payments Summit, Columbia Business School*, New York, NY, June 2017.
31. Webinar: Trends and Challenges in Mobile Money and Mobile Banking Application Security. *Digital Financial Services Observatory, Columbia University*, June 2017.
32. Towards Firmware Vetting on Legacy Embedded Platforms. *10th Workshop on Fault-Tolerant Spaceborne Computing Employing New Technologies*, Albuquerque, NM, May 2017.
33. Technical Deep Dive: Foundations of Hardware-Assisted Secure Multiparty Computation with SGX. *10th Workshop on Fault-Tolerant Spaceborne Computing Employing New Technologies*, Albuquerque, NM, May 2017.
34. Security and Privacy Challenges for Mobile Money Applications. *ITU Digital Financial Services Workshop: Exploring Innovation in Transactions and Financing in the Caribbean*, Port of Spain, Trinidad and Tobago, April 2017.
35. Everybody Jammin' Up on Those Tings: Challenges for the Internet of Insecure Things. *Forum on Internet of Things: Smarter Living in the Caribbean*, Port of Spain, Trinidad and Tobago, April 2017.
36. Application Security for DFS Applications. *ITU Workshop on DFS and Financial Inclusion*, Washington, DC, April 2017.
37. **Keynote Address:** Making USB Safer for Hosts and Peripherals. *Computer Science Research Day, University of Georgia*, Athens, GA, April 2017.
38. Security in the DFS Ecosystem - Final Recommendations. *ITU Focus Group Meeting on Digital Financial Services*, Geneva, Switzerland, December 2016.
39. Making USB Great Again: New Defenses for Hosts and Devices. *MIT Lincoln Laboratory*, Lexington, MA, USA, October 2016.
40. Making USB Great Again: New Defenses for Hosts and Devices. *Dartmouth College*, Hanover, NH, USA, October 2016.

41. Recommendations for Securing Digital Finance. *ITU Focus Group Meeting on Digital Financial Services*, Dar es Salaam, Tanzania, September 2016.
42. Secure and Efficient Data Provenance. *DARPA Transparent Computing PI Meeting*, Cambridge, MA, USA, July 2016.
43. Security for Digital Alternative Data and SME Supply Chain Finance. *G20 Global Partnership for Financial Inclusion (GPFI) Forum*, Chengdu, China, July 2016.
44. Privacy-Preserving Computing Made Practical. *9th Workshop on Fault-Tolerant Spaceborne Computing Employing New Technologies*, Albuquerque, NM, USA, June 2016.
45. Host Fingerprinting for Identity and Integrity Assurance Using Machine Learning. *9th Workshop on Fault-Tolerant Spaceborne Computing Employing New Technologies*, Albuquerque, NM, USA, June 2016.
46. Security and Privacy Challenges for Mobile Money in Mobile Devices. *5th Columbia Business School Digital Financial Services and Emerging Payments Summit*, New York, NY, USA, May 2016.
47. Trustworthy Collection Architectures for Data Provenance. *Concordia University*, Montreal, QC, Canada, May 2016.
48. Analyzing the Security of Sticky SIMs. *ITU Focus Group Meeting on Digital Financial Services*, Washington, DC, USA, April 2016.
49. Secure and Trustworthy Computers, Devices, and Systems. *South Carolina Governer's School for Science and Mathematics*, Harstville, SC, USA, December 2015.
50. Security Recommendations for the DFS Ecosystem. *ITU Focus Group Meeting on Digital Financial Services*, Geneva, Switzerland, December 2015.
51. Securing Storage for Insider Threat Mitigation. *Florida Cyber Consortium Research Symposium*, Tampa, FL, USA, October 2015.
52. Tales From the Crypt(o): Spooky Stories of Ideal-World Cryptography Meeting Real-World Implementation. *University of Calgary*, Calgary, AB, Canada, November 2015.
53. Vulnerability Analysis of Branchless Banking Apps in the Developing World. *ITU Focus Group Meeting on Digital Financial Services*, Kuala Lumpur, Malaysia, October 2015.
54. New Trends in Cybersecurity: Securing Critical Cyber-Infrastructure. *US Department of State/Department of Justice Cybercrime and Cybersecurity Workshop for Lusophone Africa*, Maputo, Mozambique, September 2015.
55. Trustworthy Collection Architectures for Data Provenance. *MIT Lincoln Laboratory*, Lexington, MA, USA, August 2015.
56. Be Who You Are: Establishing Host Identity in Local and Remote Systems. *EURECOM Institute*, Sophia Antipolis, France, July 2015.
57. Be Who You Are: Establishing Host Identity in Local and Remote Systems. *Symantec Research Labs*, Mountain View, CA, USA, April 2015.
58. Be Who You Are: Challenges of Establishing Host Identity in Local and Remote Systems. *Rutgers University*, New Brunswick, NJ, USA, March 2015.
59. Certificate Validatation and the Future of SSL Security. *Chi Sigma IO, University of Florida*, Gainesville, FL, USA, November 2014.

60. Forced Perspectives: Evaluating an SSL Trust Enhancement at Scale. *2014 ACM Internet Measurement Conference (IMC'14)*, Vancouver, BC, Canada, November 2014.
61. USB Host Fingerprinting. *Lockheed Martin*, Orlando, FL, October 2014.
62. Improving Security Through Collaborative Frameworks. *IEEE CollaborateCom (Invited Panelist)*, Miami, FL, October 2014.
63. Establishing Host Identity in Systems and Storage. *University of Florida*, Gainesville, FL, April 2014.
64. Establishing Host Identity Through Indirect Measurement. *Pennsylvania State University*, University Park, PA, April 2014.
65. **Keynote Address:** Trust No One? Addressing the Challenges of Bottom Up Trust in Systems and Storage. *Symantec Cutting Edge*, Springfield, OR, March 2014.
66. Leveraging Emerging Storage Functionality for New Security Services. *Oregon State University*, Corvallis, OR, June 2012.
67. Protecting Portable Storage with Host Validation. *Queen's University*, Kingston, ON, Canada, April 2012.
68. Protecting Portable Storage with Host Validation. *NSERC ISSNet Security Workshop*, Kingston, ON, Canada, April 2012.
69. Attacks and Defenses Against the Cloud Infrastructure. *Oregon Security Day*, Eugene, OR, April 2012.
70. Leveraging Emerging Storage Functionality for New Security Services. *Portland State University*, Portland, OR, November 2011.
71. Leveraging Emerging Storage Functionality for New Security Services. *Galois*, Portland, OR, August 2011.
72. Securing Homecare Rehabilition Environments. *UW/MSR Research Retreat*, Cle Elum, WA, August 2011.
73. Challenges and Alternatives to the Host Identification Problem. Oregon Security Day, Eugene, OR, April 2011.
74. Porscha: Policy Oriented Secure Content Handling in Android. *ACSAC 2010*, Austin, TX, December 2010.
75. Kells: A Protection Framework for Portable Data. *ACSAC 2010*, Austin, TX, December 2010.
76. Protection Mechanisms for Portable Devices. *Symantec Research Labs*, Mountain View, CA, November 2010.
77. Challenges and Alternatives to the Host Identification Problem. *2nd ACM Northeast Forensics Exchange (NeFX2010)*, Washington, DC, September 2010.
78. Disk-Enabled Authenticated Encryption. *MSST 2010*, Incline Village, NV, May 2010.
79. Leveraging Emerging Storage Functionality for New Security Services. *Polytechnic Institute of New York University*, Brooklyn, NY, March 2010.
80. Leveraging Emerging Storage Functionality for New Security Services. *Simon Fraser University*, Surrey, BC, Canada, March 2010.

81. Leveraging Emerging Storage Functionality for New Security Services. *Stevens Institute of Technology*, Hoboken, NJ, March 2010.
82. Leveraging Emerging Storage Functionality for New Security Services. *University of Tennessee*, Knoxville, TN, March 2010.
83. Leveraging Emerging Storage Functionality for New Security Services. *University of Oregon*, Eugene, OR, March 2010.
84. Leveraging Emerging Storage Functionality for New Security Services. *Naval Postgraduate School*, Monterey, CA, February 2010.
85. Towards a Secure and Efficient System for End-to-End Provenance. *TaPP'10*, San Jose, CA, February 2010.
86. Rootkit-Resistant Disks. *Security Reading Group, University of Toronto*, Toronto, ON, Canada, November 2009.
87. Rootkit-Resistant Disks. *Digital Security Seminar, Carleton University*, Ottawa, ON, Canada, November 2009.
88. U Can't Touch This: Protections for Portable Storage. *IWSSPS 2009*, Grenoble, France, Oct. 2009.
89. FlowStor: Preserving Information Flow on Portable Storage Devices. *Symantec Corporation*, Mountain View, CA, USA, August 2009.
90. Leveraging Emerging Disk Functionality for New Security Services. *Symantec Research Labs*, Mountain View, CA, USA, June 2009.
91. Rootkit-Resistant Disks. *CCS'08*, Alexandria, VA, USA, October 2008.
92. Experimenting with BGP Security Mechanisms Using the DETER Framework. *Boeing Integrated Defense*, Philadelphia, PA, USA, October 2008.
93. Terabyte Home Security and Access Control. *Seagate Research*, Pittsburgh, PA, USA, August 2008.
94. Towards Automated Privilege Separation. *ICISS 2007*, Delhi, India, December 2007.
95. Non-Volatile Memory and Disks: Avenues for Policy Architectures. *CSAW 2007*, Fairfax, VA, USA, November 2007.
96. Autonomously Secure Disks. *Software Reading Group, University of Michigan*, Ann Arbor, MI, USA, September 2007.
97. Leveraging Non-Volatile Memory for Storage Security. *2007 USENIX Security Symposium, Works in Progress*, Boston, MA, USA, August 2007.
98. Analysis of the IPv4 Address Delegation Structure. *ISCC 2007*, Aveiro, Portugal, July 2007.
99. Performance Optimizations of IPsec for Storage. *2007 SNIA Summer Security Summit*, Pittsburgh, PA, June 2007.
100. Optimizing BGP Security by Exploiting Path Stability. *CCS'06*, Alexandria, VA, November 2006.
101. Threats and Attacks in Interdomain Routing. *P2INGS Quarterly Meeting*, Tempe, AZ, February 2004.
102. Network Operations in Tier-1 Internet Service Providers. *Columbia University*, New York, NY, March 2001.
103. Network Operations in Tier-1 Internet Service Providers. *Telcordia Technologies*, Morristown, NJ,

August 2000.

Press Coverage

Research-Related Coverage

1. "Exploiting Decades-Old Telephone Tech to Break Into Android Devices." Lily Hay Newman, *Wired*, August 29, 2018. https://www.wired.com/story/at-commands-android-vulnerability/

2. "Modern smartphones vulnerable to old-school attack." Francis Navarro, *Komando.com*, August 28, 2018. https://www.komando.com/happening-now/483269/modern-smartphones-vulnerable-to-old-school-attack

3. "ATak na Androida: modemowe komendy standardu z lat 80 pozwalają przejąć kontrolę nad smartfonem" (Translation from Polish: "ATtack on Android: modem commands from the 80's standard allow you to take control of your smartphone".) Adam Golanski, *Dobreprogramy*, August 28, 2018. https://www.dobreprogramy.pl/ATak-na-Androida-modemowe-komendy-standardu-z-lat-80-pozwalaja-przejac-kontrole-nad-smartfonem,News,90526.html

4. "Смартфоны ASUS, HTC, Huawei, Lenovo, LG, Samsung, Sony легко взломать технологией, созданной для древнего модема Подробнее" (Translation from Russian: "Smartphones ASUS, HTC, Huawei, Lenovo, LG, Samsung, Sony can easily crack technology created for the ancient modem.") Roman Georgiev, *CNews Russia*, August 28, 2018. http://safe.cnews.ru/news/top/2018-08-28_smartfony_asushtchuaweilenovolgsamsungsony

5. "AT Command Hitch Leaves Android Phones Open to Attack." Lindsey O'Donnell, *Threatpost*, August 27, 2018. https://threatpost.com/at-command-hitch-leaves-android-phones-open-to-attack/136938/

6. "New security risk for smartphones bring you a 'ghost user'." Ida Torres, *Android Community*, August 27, 2018. https://androidcommunity.com/new-security-risk-for-smartphones-brings-you-a-ghost-user-20180827/

7. "Android at the mercy of AT commands." Nick Farrell, *Fudzilla*, August 27, 2018. https://fudzilla.com/news/mobile/47037-android-at-the-mercy-of-at-commands

8. "Android-Smartphones durch Modem-Befehle verwundbar" (Translation from German: "Android Smartphones vulnerable through modem commands".) Sebastian Gruner, *Golem.de: IT-News Für Profis*, August 27, 2018. https://www.golem.de/news/at-commands-android-smartphones-durch-modem-befehle-verwundbar-1808-136205.html

9. "Telefony s Androidem lze ovládnout přes USB pomocí AT příkazů"(Translation from Czech: "Android phones can be controlled via USB using AT commands"). Petr Krcmar, *Root.cz Linux News*, August 27, 2018. https://www.root.cz/clanky/telefony-s-androidem-lze-ovladnout-pres-usb-pomoci-at-prikazu/

10. "У 11 производителей Android-смартфонов обнаружили уязвимость к AT-командам" (Translation from Russian: "11 manufacturers of Android-smartphones found a vulnerability to AT-commands".) *Tproger*, August 27, 2018. https://tproger.ru/news/at-commands-deface-smartphones/

11. "Smartphones From 11 OEMs Vulnerable to Attacks via Hidden AT Commands." Catalin Cimpanu,

Bleeping Computer, August 25, 2018. https://www.bleepingcomputer.com/news/security/smartphones-from-11-oems-vulnerable-to-attacks-via-hidden-at-commands/

12. "Smartphone security risk compared to 'having a ghost user on your phone'." Jonathan Griffin, *University of Florida News*, August 22, 2018. http://news.ufl.edu/articles/2018/08/smartphone-security-risk-compared-to-having-a-ghost-user-on-your-phone.php
13. "Ransomware 'stopped' by new software." *BBC News*, July 2016. http://www.bbc.com/news/technology-36772461
14. "United States and Mozambique Host Cybersecurity and Cybercrime Workshop in Maputo for Lusophone Africa." *US Department of State*, September 2015. http://www.state.gov/r/pa/prs/ps/2015/09/247088.htm
15. "Researchers Find Security Flaws in Developing-World Money Apps." Jennifer Valentino-Devries. *Wall Street Journal*, August 2015. http://blogs.wsj.com/digits/2015/08/11/researchers-find-security-flaws-in-developing-world-money-apps/
16. "Hack could let browsers use cloud to carry out big attacks on the cheap." Dan Goodin, *Ars Technica*, November 2012. http://arstechnica.com/security/2012/11/hack-could-let-browsers-use-cloud-to-carry-out-big-attacks-on-the-cheap/

Other Coverage

17. "Voters in Two States Report Threatening 'Vote for Trump' Emails", Nick Corasanitti, Ben Decker, and Stephanie Saul, *The New York Times*, 20 October 2020. https://www.nytimes.com/2020/10/20/us/politics/florida-alaska-trump-emails.html
18. "What Would It Take to Shut Down the Entire Internet?" Daniel Kolitz, *Gizmodo*, 30 September 2019. https://gizmodo.com/what-would-it-take-to-shut-down-the-entire-internet-1837984019
19. "Devious Ransomware Frees You If You Infect Two Other People." Lily Hay Newman, *Wired*, 13 December 2016. https://www.wired.com/2016/12/popcorn-time-ransomware/
20. "UF experts: iPhone issue could set precedent." Christopher Curry and Dahlia Ghabour, *Gainesville Sun*, 26 February 2016. http://www.gainesville.com/article/20160226/ARTICLES/160229743/-1/archive?Title=UF-experts-iPhone-issue-could-set-precedent
21. "Biometric Security Comes To Your Smartphone." Mitch Kroner, *Think Out Loud, Oregon Public Broadcasting*, 24 September 2013. http://www.opb.org/radio/programs/thinkoutloud/segment/biometric-security-comes-to-your-smartphone/

Previous Academic Appointments

Associate Professor, Department of Computer and Information Science and Engineering, University of Florida, Aug. 2014 - Aug. 2021
Associate Director of the Florida Institute for Cybersecurty Research. Previous co-director of the Southeastern Security for Enterprise and Infrastructure Center.
Assistant Professor, Department of Computer and Information Science, University of Oregon, Sep. 2010 - Aug. 2014
Research and teaching classes in systems security. Founder and leader of the Oregon Systems

Infrastructure Research and Information Security Laboratory. Co-director of the Center for Cyber Security.

- **Leadership:** Organizer of Computer Security Day at the University of Oregon (2014, 2013, 2012, 2011, recipient of CAS program grant for three years), liaison to Oregon Engineering and Technology Council (2010-2012), faculty advisor to UO Security Club (2012-2014), faculty liaison to Women in Computer Science (2012-2013).
- **Committee Service:** University Committee on General Science Major (2014), Graduate Education Committee (2010-2012, 2014-present), Computing Resources Committee (2011-2012), Industrial Affairs Committee (2012-2014), Strategic Planning Committee (2013).

Research Assistant, Department of Computer Science, Pennsylvania State University, Jan. 2005 - Aug. 2010

- **Senior Personnel**, NSF HECURA: Collaborative Research: Secure Provenance in High-End Computing Systems, NSF (CCF), $307,073, Aug. 2009 - present.
- Funded by NSF HECURA grant 0621429 from Aug. 2006 - Jul. 2010, investigating security of storage systems.
- Funded by NSF grant CNS-0335241 from Aug. 2005 - Aug. 2006, investigating BGP security solutions and large-scale simulation.

Lead Graduate Student, Systems and Internet Infrastructure Security (SIIS) Laboratory, Pennsylvania State University, Sep. 2007 - Dec. 2008

- Administrative and logistical lead student in the SIIS lab. Ran weekly lab meetings of 13 members, met with students individually for mentoring and development of leadership and research skills. Responsible for most daily operational activities in the lab.

Instructor, Department of Electrical Engineering, Pennsylvania State University, Jun.-Aug. 2006

- Instructor for *EE/CSE 458,* the senior undergraduate course on computer networking.

Guest Lecturer, Department of Computer Science, Pennsylvania State University, 2005-present

- *CSE 543 (Computer Security):* presented lectures on cryptography and public key infrastructures.
- *CSE 597A (Advanced Topics in System Security):* lectured on virtual machine security.
- *CSE 411 (Operating Systems):* presented lectures on storage systems.
- *CSE 545 (Advanced Network Security):* lectured on BGP security.

Teaching Assistant, Stern School of Business, New York University, Fall 2005

- Lectured, graded, and provided logistics for Computer and Network Security course offered for MBA students.

Teaching Assistant, Department of Computer Science and Engineering, Pennsylvania State University, Fall 2004

- Held lab hours and graded for Computer System Architecture course.

Graduate Research Assistant, Department of Computer Science, Columbia University, Oct. 2001 - May 2002

- Worked on SIP security, implementing authentication into the Panasonic PINTL JAIN SIP stack.

Teaching Assistant, Department of Computer Science, Queen's University, Fall 1998

- Held office hours and graded for Introduction to Computer Science course.

Industrial Experience

Co-Founder and Chief Operating Officer, CryptoDrop LLC, 2017-2019.

- Anti-ransomware startup based in Gainesville, Florida.

Research Intern, Symantec Research Labs, Mountain View, CA, Jun - Aug. 2009

- Examined host-based validation for portable storage devices, and implemented a prototype using embedded Linux.

Research Intern, Seagate Research, Pittsburgh, PA, May - Aug. 2008

- Developed security infrastructures for distributed storage in a home user environment, focussing on distributed access control mechanisms.

Research Intern, AT&T Labs - Research, Florham Park, NJ, Dec. 2003 - Aug. 2004

- Investigated security threats in BGP and created an overview of threats and currently deployed solutions. Developed cryptographic constructions allowing efficient security solutions and performed simulations based on trace data.

Technical Intern, Flarion Technologies, Bedminster, NJ, Summer 2002

- Implemented packet diversion and IP header modification program in BSD for mobile IP packet testing.

Research Scientist, Telcordia Technologies, Morristown, NJ, Sep. 2000 - Nov. 2001

- Built and maintained an HFC lab to emulate a cable plant; researched routing and service assurance methodologies for multiple service providers acessing common transport.

Technical Specialist, UUNET, Toronto, ON, May 1999 - Aug. 2000

- Monitored and troubleshot intermediate and backbone connections across the UUNET Canadian network, as well as dealing with network security and web server issues.

Summer Intern, Royal Bank of Canada, Toronto, ON, Summer 1997, 1998

- Investigated financing opportunities for life science and high tech companies through financial and technical analysis; ported applications from mainframe to client-server environments.